Nom du document	Version	Date de MAJ	Auteure	Contenu
Stormshield Bases - Fiches1a4.docx	1.0	14/09/2020	V Martinez	Cours issu du support CSNA v4 Routage, NAT, Filtrage Lab 1 à 5

Support de formation réalisé dans le cadre du partenariat Stormshield Académie avec le réseau national Certa

Table des matières

Table des matières 1
Phase 1 Prise en main – configuration initiale 3
1.1 - Connexion au pare-feu SNS 4
1.2 - Interface d'administration du pare-feu SNS 5
1.3 - Configuration générale 7
1.4 - Traces et Journaux 11
Phase 2 Mise en place du plan d'adressage réseau 13
2.1 - Configuration des interfaces réseau 13
2.2 - Route par défaut 15
2.3 - Mise en œuvre de la traduction d'adresses pour l'accès à Internet (NAT/PAT) 15
Phase 3 Configuration des Objets Réseau 20
3.1 - Présentation des Objets 20
3.2 - Création des Objets Réseaux 21
3.3 - Import/Export des Objets Réseaux 24
Phase 4 Traduction d'adresses (NAT/PAT) 26
4.1 - Mise en œuvre de la NAT statique 26
4.2 - Mise en œuvre de la redirection de ports 27
4.3 - Traçage des règles de NAT 27
4.4 - Export des règles de NAT 28
Phase 5 Filtrage protocolaire 29
5.1 - Présentation des fonctionnalités 29
5.2 - Mise en place des règles de filtrage 30
Annexe – Procédure de Remise à zéro des Pare-feux SNS 34

I Présentation du document

Objectif du document

Ce support comporte des fiches pratiques de travaux en laboratoire permettant d'exploiter les pare-feux Stormshield SNS virtuels ou physiques dans le cadre du bloc 3 sur la cybersécurité.
Il est basé sur les documents et les laboratoires de la formation officielle Stormshield pour les formations CSNA et CSNE et réalisé dans le cadre du partenariat Stormshield Académie avec le réseau national Certa.

Utilisation du document

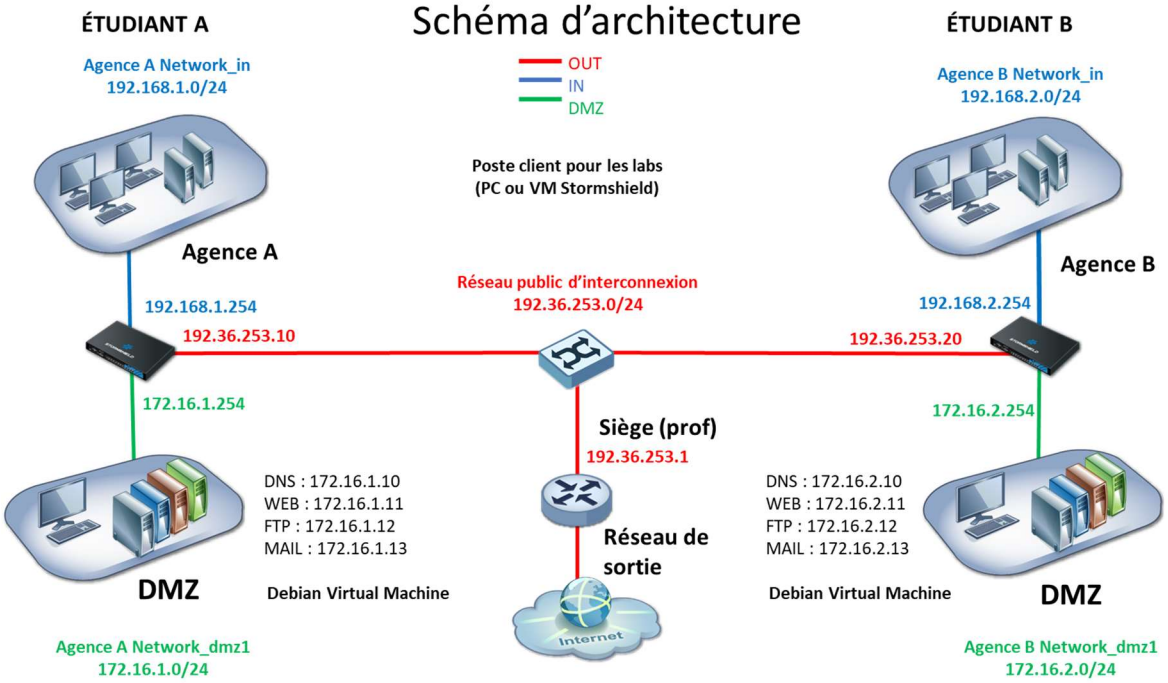
Chaque fiche pratique est un exemple destiné à aborder certaines compétences du bloc 3. Les professeurs peuvent reprendre, en l'état, ces fiches pratiques ou les modifier pour les intégrer dans leurs travaux en laboratoire. Le support vise l'option SISR et comporte plusieurs fiches en fonction du thème abordé.

II Présentation de l'architecture du laboratoire

Stormshield, dans le cadre du partenariat avec le réseau Certa fournit gratuitement les machines virtuelles de la plateforme (le parefeu Stormshield SNS, un client linux, le serveur DMZ) exploitables directement en autonomie sur virtual box (2 agences et le « siège »), ou après conversion sur un hyperviseur pour l'ensemble des étudiants. Nous nous placerons dans ce second cas où chaque étudiant gère une agence reliée via un réseau public d'interconnexion factice aux autres agences et au parefeu de l'enseignant. Si l'établissement possède des boitiers physiques, l'infrastructure sera identique. Si vous utilisez les kits en autonomie, reportez-vous à la documentation d'installation des labs fournie par Stormshield pour les aspects réseaux virtuels.
Dans la suite du texte le terme pare-feu SNS concerne l'appliance virtuelle ou le boîtier physique Stormshield. L'architecture proposée (issue du kit de formation CSNA Stormshield) est constituée de plusieurs agences (A, B, C…) correspondant à un étudiant et d'un siège géré par l'enseignant. Chaque agence possède une plateforme composée d'un pare-feu SNS Stormshield (physique ou virtuel), d'une machine cliente (physique ou virtuelle), d'une machine serveur Debian préconfigurée avec des services accessibles en DMZ.
Chaque agence comporte un réseau interne privé **IN,** une **DMZ** et un réseau d'interconnexion **OUT** (simulant le WAN) relié au siège de l'entreprise où le pare-feu SNS Siège est configuré pour permettre l'accès à Internet des agences via le réseau du BTS SIO.

Fiche pratique n°1 : Configuration de base avec NAT/PAT accès Internet

Le schéma ci-dessous représente l'architecture avec 2 agences et le siège.



Chaque agence est composée :

- ❖ d'un réseau externe **OUT** « 192.36.253.x0/24 » auquel les firewalls de toutes les agences sont connectés relié à l'interface **OUT** du pare-feu SNS ;
- ❖ d'un réseau interne **IN** Agence x « 192.168.x.0/24 » relié à l'interface **IN** du pare-feu SNS avec un poste utilisateur : machine virtuelle cliente Kali fournie ou autre VM ;
- ❖ d'un réseau **DMZ1** « 172.16.x.0/24 » avec des services (DNS, WEB, FTP, MAIL) intégrés dans la machine virtuelle Debian serveur fournie dans le kit Stormshield CSNA ;
- ❖ d'un réseau **DMZ2** d'administration en DHCP relié au LAN BTS SIO interne accessible depuis une machine physique du BTS SIO sans modification de configuration.

L'architecture ci-dessus peut être étendue à plus de participants en respectant le plan d'adressage ci-dessous.

m0	**OUT** : Réseau d'interconnexion « 192.36.253.x0 /24 »	@Interface **OUT** 192.36.253.x0 /24
em1	**IN** : Réseau interne Agencex « 192.168.x.0/24 »	@Interface **IN** 192.168.x.254 /24
em2	**DMZ1** : Réseau DMZ « 172.16.x.0/24 »	@Interface **DMZ1** 172.16.x.254 /24
em3	**DMZ2** : Réseau d'administration (LAN BTS SIO)	@Interface **DMZ2** DHCP

Il suffira de modifier le « **x** » suivant la lettre de l'agence **A⇒1**, B⇒2, C⇒3, D⇒4...

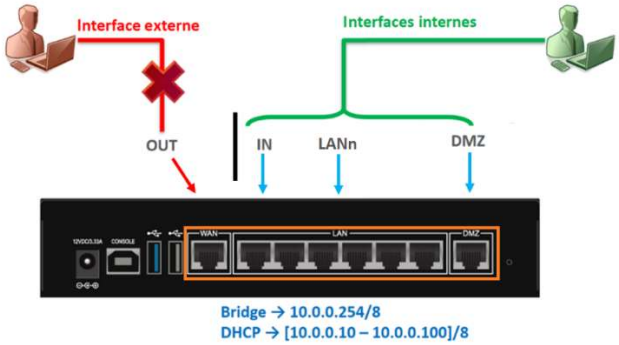
Phase 1 Prise en main – configuration initiale

Avertissement : les manipulations décrites ici peuvent être complétées par celles décrites dans le chapitre Prise en main du firewall (p40) du support de cours CSNA Stormshield.

La configuration d'usine par défaut du *pare-feu SNS* (boîtier ou appliance VM laboratoire) est la suivante.

Dans une configuration usine, la première interface du pare-feu SNS physique est nommée « OUT », la seconde « IN » et le reste des interfaces « DMZx ». L'interface « OUT » est une interface **externe**, utilisée pour connecter le pare-feu SNS à internet et le reste des interfaces sont **internes** et servent principalement à connecter le pare-feu SNS à des réseaux locaux.

La distinction interne/externe pour les interfaces permet de se protéger contre les attaques d'usurpation d'adresse IP.



Sur un boitier physique (et les VM individuelles virtualbox de labo), toutes les interfaces sont incluses dans un bridge dont l'adresse est 10.0.0.254/8. Un serveur DHCP est actif sur toutes les interfaces du bridge et il distribue des adresses IP comprises entre 10.0.0.10 et 10.0.0.100. L'accès à l'interface web de configuration du pare-feu SNS se fait avec l'url : **`https://10.0.0.254`**
Par défaut, seul le compte système **admin** (mot de passe par défaut **admin**), disposant de tous les privilèges sur le boîtier, existe et peut se connecter.
Remarque : Sur une VM installée sur une ferme de serveurs, il est recommandé d'utiliser le mode de remise à zéro de la configuration pour lancer un dialogue de pré-configuration qui va vous demander de changer le mot de passe par défaut (8 caractères et Maj/min demandé), de configurer vos interfaces, le clavier de la console… La manipulation est décrite en annexe de ce document.

1.1 - Connexion au pare-feu SNS

Pour accéder à l'interface d'administration du pare-feu SNS, il est indispensable de connecter votre machine sur une interface interne (**IN** ou **DMZ1 ou 2**) sous peine de devoir redémarrer le firewall qui aura détecté une tentative d'usurpation d'adresse IP sur le bridge et bloquera tout le trafic généré par la machine connectée sur l'interface **OUT**.
Pour faciliter la mise en place de la configuration initiale du pare-feu SNS, nous travaillerons sur une interface en DMZ (**DMZ2** si elle existe) qui sera momentanément relié à une machine physique soit en direct sur le boitier soit sur une ferme de serveurs via le réseau local du BTS SIO.

- Vérifiez que votre machine hôte a bien obtenu une adresse IP dans la plage 10.0.0.**0/24**, ou sur le réseau du BTS SIO, le cas échéant la configurer manuellement.

L'accès à l'interface graphique d'administration du pare-feu SNS se fait par https://10.0.0.254/admin à partir d'un navigateur web (de préférence Firefox, Chrome ou Edge)
Au premier démarrage d'un boitier pare-feu SNS physique, un écran de configuration rapide vous est proposé, dans la zone **Options** en bas de l'écran choisissez la langue **Français**, ressaisissez le mot de passe : **admin** puis dans la zone en bas sélectionnez **Accès direct à l'interface d'administration** qui vous permet de ne pas exécuter l'assistant de configuration.
NB : pour des raisons évidentes de sécurité, il conviendra de modifier ce mot de passe lorsque le pare-feu SNS sera utilisé en contexte réel d'entreprise.

L'écran ci-contre apparaît pour vous connecter une fois le pare-feu SNS démarré.

- Pour modifier les options de langue de l'interface web d'administration, dépliez **Options** puis choisissez la langue.

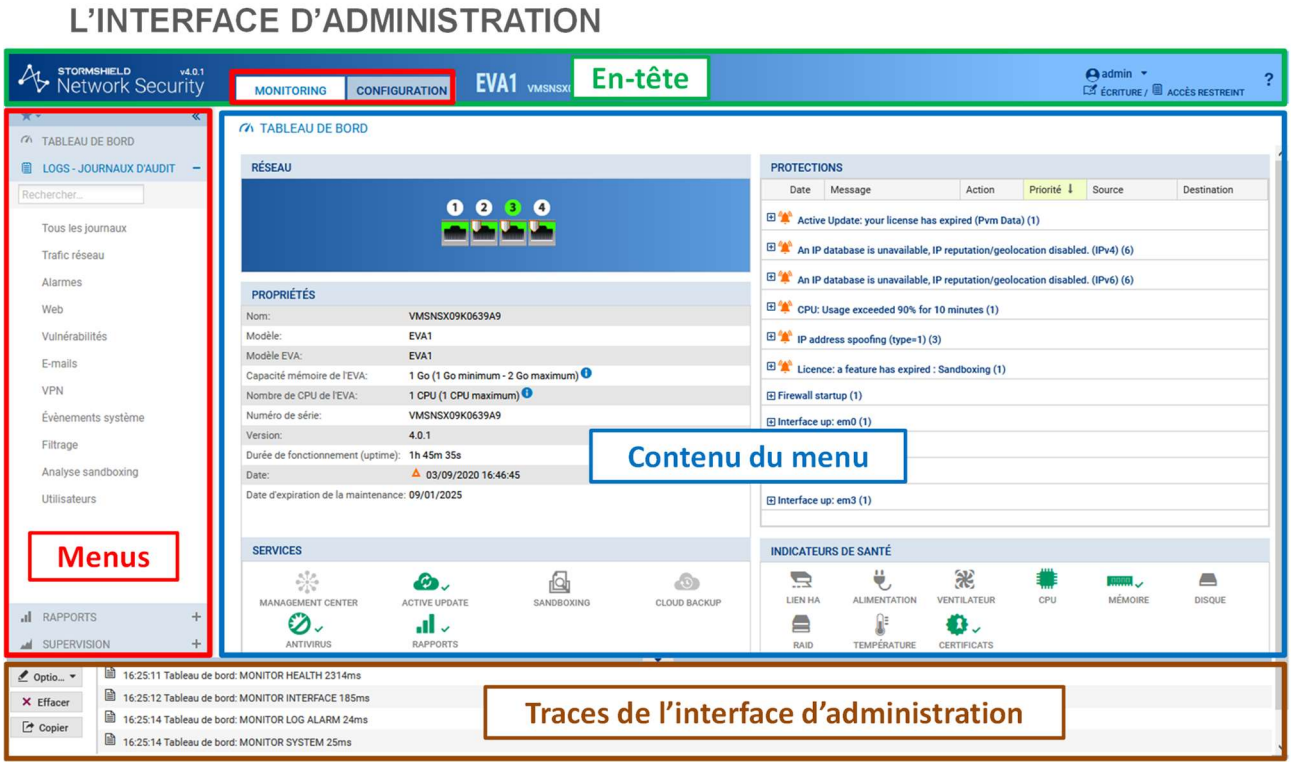
La fenêtre est actualisée, vous pouvez vous connecter.

- Saisir l'identifiant **admin,** le mot de passe **admin** ou celui que vous avez configuré lors de la réinitialisation de la machine virtuelle (**SioSioSio** ou autre)

Pour s'authentifier, l'utilisateur peut également sélectionner un certificat dans le magasin de son navigateur (à configurer au préalable dans les préférences du pare-feu SNS).

1.2 - Interface d'administration du pare-fu SNS

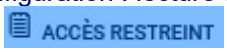
La page d'accueil de votre pare-fu SNS s'ouvre sur **`Tableau de bord`** qui permet de visualiser un certain nombre d'informations sur votre équipement et est personnalisable.



L'interface d'administration est découpée en quatre parties :

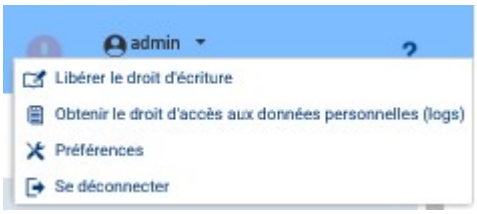
1. **L'en-tête (partie encadrée en vert) :** Elle contient les informations suivantes :
   - Le **nom** du pare-feu SNS : le nom par défaut est le numéro de série,
   - La **version du système** (firmware),

   - **L'utilisateur connecté** sur l'interface, ses droits d'accès à la configuration : lecture seule ou écriture 

et ses droits d'accès aux logs : restreint 

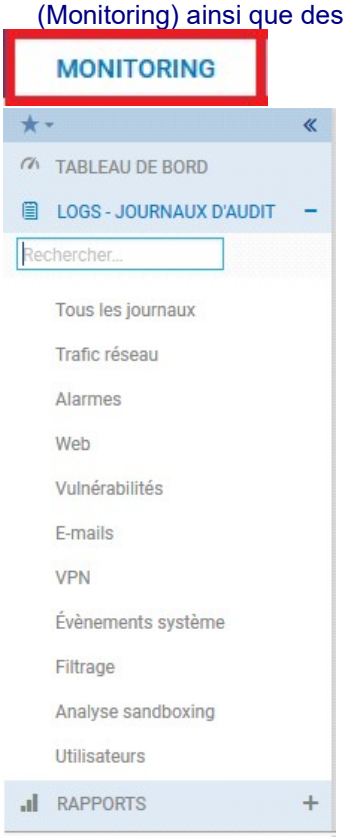
ou complet,
   - Un lien vers **l'aide en ligne** du menu courant ainsi que des informations complémentaires sur les paramètres et les options du menu.

Cliquez sur la flèche à droite du nom d'utilisateur (admin) permet d'accéder à plusieurs fonctionnalités :



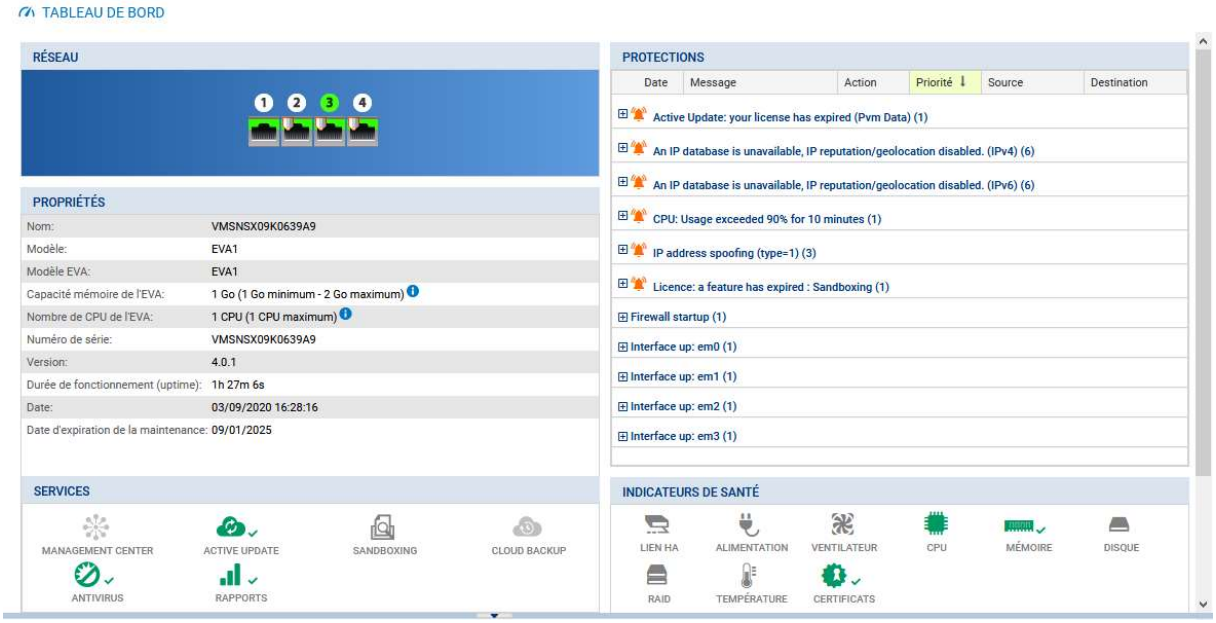
   - Acquérir ou **libérer le droit d'écriture**. Notez qu'à un instant donné, un seul utilisateur peut disposer du droit d'écriture sur le pare-feu SNS ;
   - **Obtenir le droit d'accès aux données personnelles** ;
   - Le menu « **Préférences** » permet de configurer plusieurs paramètres en relation avec l'interface d'administration. Les plus importants sont :
     - Le **temps d'inactivité** avant de déconnecter l'utilisateur de l'interface d'administration (30 minutes par défaut) ;
     - Les options d'affichage dans les menus (toujours afficher les configurations avancées, nombre de règles de filtrage par page, etc.) ;
     - Liens externes vers les sites Stormshield
   - **Se déconnecter** : déconnecte l'utilisateur courant.

2. **Les menus (partie encadrée en rouge) :** Regroupe les menus de configuration, de supervision (Monitoring) ainsi que des raccourcis organisés sous forme de listes rétractables.



Les menus sont séparés en 2 catégories qui s'affichent ensuite sur la zone de menu de gauche constituée d'un ensemble de panneaux qui permettent d'accéder aux différents menus de votre pare-feu SNS.
L'onglet **Monitoring** pour tout ce qui touche à la supervision, les log et l'état du pare-feu SNS. L'onglet **configuration** pour les objets et le paramétrage des diverses fonctionnalités.

3. **Le contenu du menu (partie encadrée en bleu) :** Affiche le contenu du menu sélectionné.
4. **Les traces de l'interface d'administration (partie encadrée en marron) :** Affiche une liste (paramétrable) des logs de l'interface web. On peut y faire apparaitre par exemple les commandes NSRPC exécutées par l'interface web, les erreurs levées, les avertissements, ….



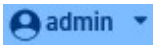
Le **`Tableau de bord`**, regroupe l'ensemble des informations et indicateurs du pare-feu SNS :

- ❖ État du module Active Update ;
- ❖ Alarmes ;
- ❖ Licence (date d'expiration de chaque module),
- ❖ Propriétés (N° de série, politiques actives, date et heure…) ;
- ❖ Interfaces (listing des interfaces réseau configurées) ;
- ❖ État des différents services.

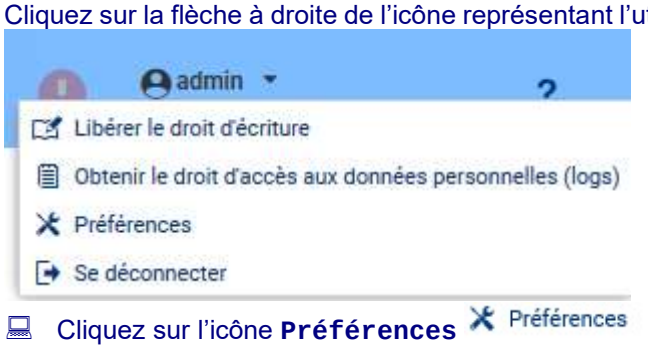
Un clic sur un élément du tableau de bord renvoie directement vers la page de supervision ou de configuration liée à cet élément.

1.3 - Configuration générale

Nous verrons ci-après un certain nombre d'éléments de configuration générale utiles pour la bonne mise en œuvre de votre pare-feu SNS. Nous étudierons notamment les éléments du menu **`Configuration / Système`** qui correspond à la configuration générale : licence, mise à jour, mot de passe...
Afin de ne jamais être déconnecté en cas d'inactivité sur l'interface d'administration pendant ces exercices pratiques, il conviendra de modifier vos préférences, en usage réel vous utiliserez un délai de 5 minutes pour éviter de laisser votre session ouverte sur le pare-feu SNS.

Cliquez sur la flèche à droite de l'icône représentant l'utilisateur connecté 

en haut à droite.

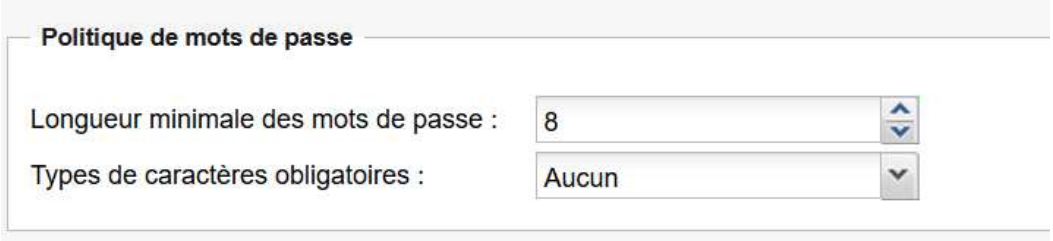


- Cliquez sur l'icône **`Préférences`**

- Dans la zone **`Paramètres de connexion`**, sélectionnez dans la liste "Déconnexion en cas d'inactivité :" la valeur Toujours rester connecté.

- Sélectionnez dans le menu à gauche **`Configuration / Système`** puis **`Configuration`**. Le volet **`Configuration générale`** est affiché.
- Commencez par donner un **nom** à votre boîtier : FWX_AgenceX et **changer la langue** de la console. Nous laisserons les logs en anglais.

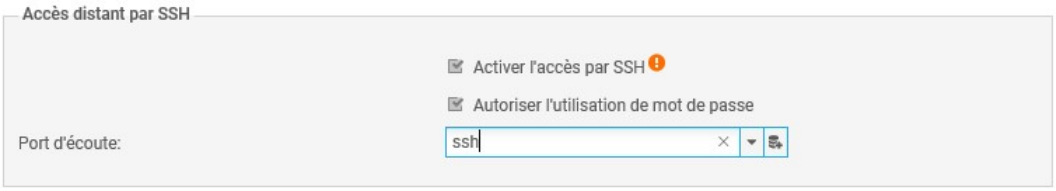
- La zone **`Politique de mots de passe`** permet de définir la longueur du mot de passe (8 par défaut) et la zone **`Types de caractères obligatoires`** permet de gérer la complexité du mot de passe (Aucun, Alphanumériques, Alphabétiques et spéciaux).

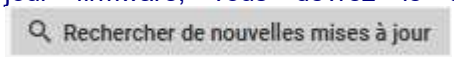


- Modifiez le fuseau horaire dans la zone **Date et heure (Europe/Paris).**
- Cliquez **Synchroniser avec votre machine** ou **Maintenir le firewall à l'heure (NTP)** pour que les mises à jour d'heure d'été/heure d'hiver soient également effectives.
- Cliquez le bouton **`Appliquer`** pour sauvegarder la configuration et **`Redémarrer plus tard`**.

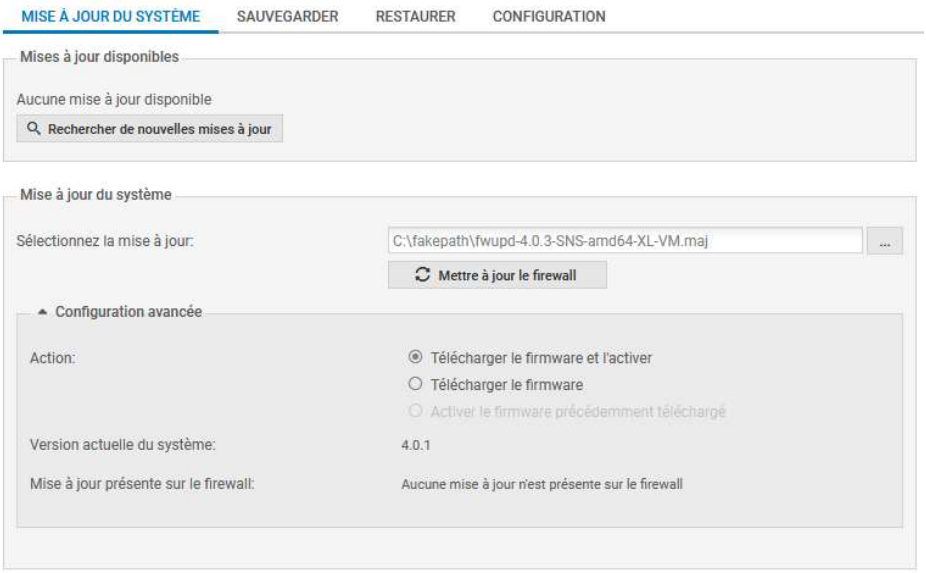
Voici quelques commandes rapides pour réaliser le paramétrage initial du pare-feu SNS.

- La **modification du mot de passe admin** (recommandée) se fait dans le menu **`Configuration / Système / Administrateurs /`** `onglet` **`Compte ADMIN.`** Le mot de passe doit par défaut, comporter au moins **5 caractères**. La force du mot de passe choisit s'affiche alors. Les boutons **`Exporter la clé privée`** et **`Exporter la clé publique du firewall`** permettent respectivement de télécharger la clé privée et clé publique du compte admin.
- La **sauvegarde de la configuration** se fait dans le menu **`Configuration / Système / Maintenance / onglet Sauvegarder`**. La sauvegarde automatique du fichier de configuration peut être mise en place et effectuée sur le Cloud Stormshield.
- L'accès SSH s'active depuis le menu **`Configuration / Système / Configuration`** onglet **`Administration du firewall`**, cocher **Activer l'accès par SSH** et **Autoriser l'utilisation de mot de passe**, puis choisir **ssh** dans Port d'écoute.



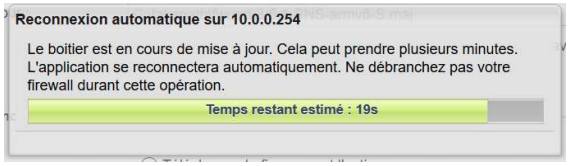
- Le menu **`Configuration / Système / Maintenance /`** `onglet` **`Mise à jour du système`** permet de mettre à jour le système le cas échéant. Afin d'appliquer un fichier de mise à jour firmware, vous devrez le télécharger sur l'UTM (soit directement via le lien  , soit en allant le télécharger sur le site https://mystormshield.eu). Nous allons procéder à la mise à jour vers la dernière version disponible que vous aurez au préalable téléchargée.

- Cliquez **`Configuration /`** Système / Maintenance / onglet Mise à jour du système.



- Sélectionnez le fichier de mise à jour présent sur votre poste de travail.
- Dépliez la zone **Configuration avancée.**
- Dans la « configuration avancée », vous pouvez choisir de **Télécharger le firmware et l'activer** ce qui appliquera la mise à jour ou bien de la télécharger uniquement, son activation pourra se faire ultérieurement avec l'option **Activer le firmware précédemment téléchargé**.
- Dans la zone **Configuration avancée** choisir Télécharger le firmware et l'activer
- Cliquez le bouton 

L'opération prendra plusieurs minutes surtout ne débranchez pas le pare-feu pendant la mise à jour. Le pare-feu sera ensuite redémarré.



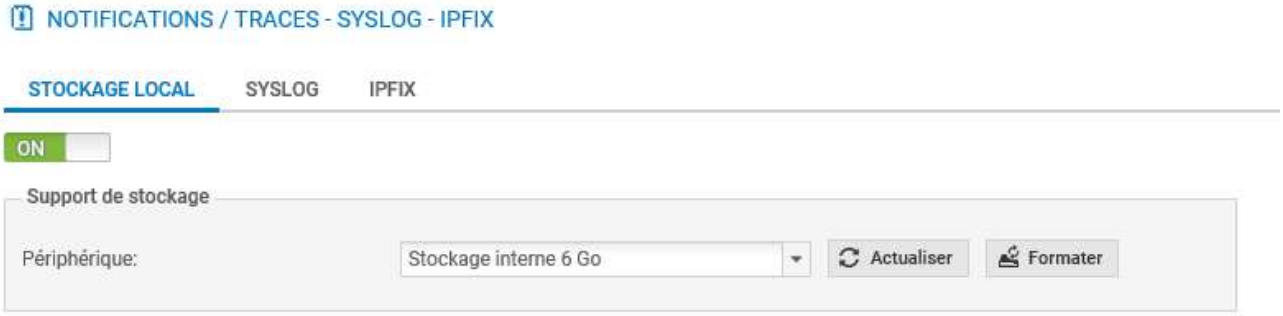
- Le menu **Configuration / Système / Maintenance /** onglet **Configuration** permet **uniquement sur les boitiers physiques** de déterminer la partition active et ainsi de garder deux versions du système disponibles avec une partition de sauvegarde qui permet de revenir en arrière sur le boitier (firmware n-1, config n-1).

NB : Pour revenir à une configuration ou version n-2 ou supérieure il faut utiliser USB Recovery.

- Le menu **Configuration / Système / Active update** permet de contrôler la mise à jour automatique des modules de Bases d'URLs embarquées, IPS : Signatures de protection contextuelles, Géolocalisation / Réputation IP publiques, signatures antispam, antivirus et autres listes noires préconfigurées par Stormshield. Vous pouvez le cas échéant les désactiver mais au contraire vérifiez qu'elles sont bien toutes activées.
- Le menu **Configuration / Système / Licence** affiche les détails de la licence et permet le cas échéant de l'installer (à récupérer par l'administrateur sur le site *mystormshield.eu* avec les informations figurant sous le boitier).
  À noter que si vous n'activez pas la licence au bout d'un certain temps les fonctionnalités se réduisent et surtout vous ne pourrez pas stocker les logs sur les boitiers physiques.

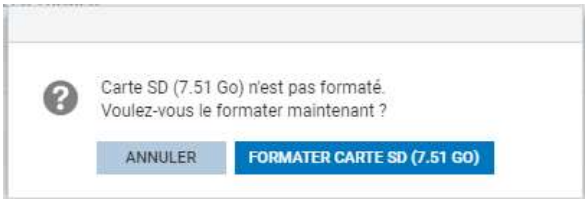
Stockage des logs : onglet **Configuration / Notifications / Traces – Syslog - IPFIX**

- L'activation du stockage local des logs s'effectue dans l'onglet **Configuration / Notifications / Traces – Syslog - IPFIX** / **Stockage local**
  Sur une machine virtuelle, celui-ci est activé par défaut et occupe un espace disque de 6Go.

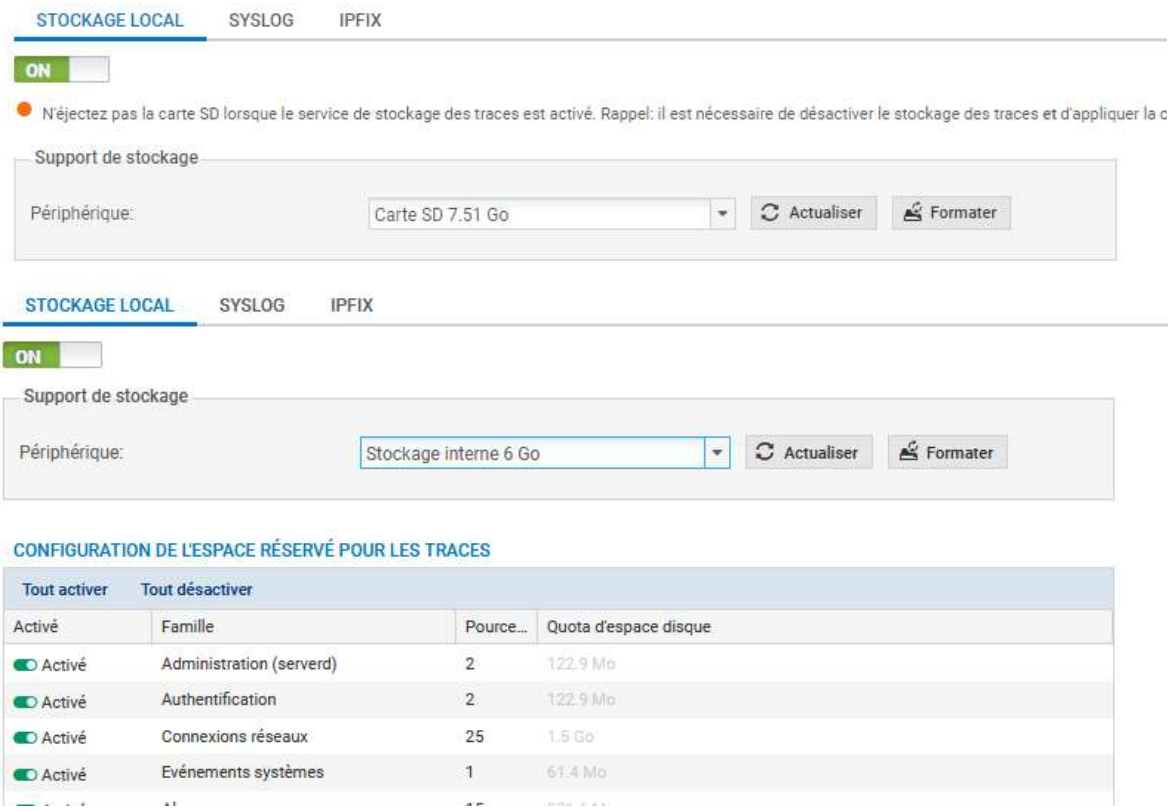


Sur un boitier physique, celui-ci n'est pas activé par défaut. Vous devez insérer une carte SD dans l'emplacement en façade du pare-feu SNS, elle sera automatiquement détectée (sauf si vous n'avez pas installé la licence) et le système vous proposera de la formater avant utilisation.

- Au besoin, cochez le bouton **ON** et dans **Périphérique** sélectionnez la carte SD comme support de stockage.



- Le système vous propose de la formater avant utilisation, cliquez **Formater Carte SD**. Cette opération prend quelques secondes.
  NB : Afin de stocker les journaux du pare-feu SNS sur un support externe (carte SD) vous devez d'abord enregistrer la licence, le message d'erreur n'est pas explicite, le système fait comme s'il ne pouvait détecter la carte SD.



Une fois formaté la liste des journaux préconfigurés est activée avec pour chaque journal un espace dédié. Vous pouvez désactiver certains journaux si vous le souhaitez.

- Le cas échéant, cliquez **Appliquer** puis **Sauvegarder** pour activer le stockage des journaux

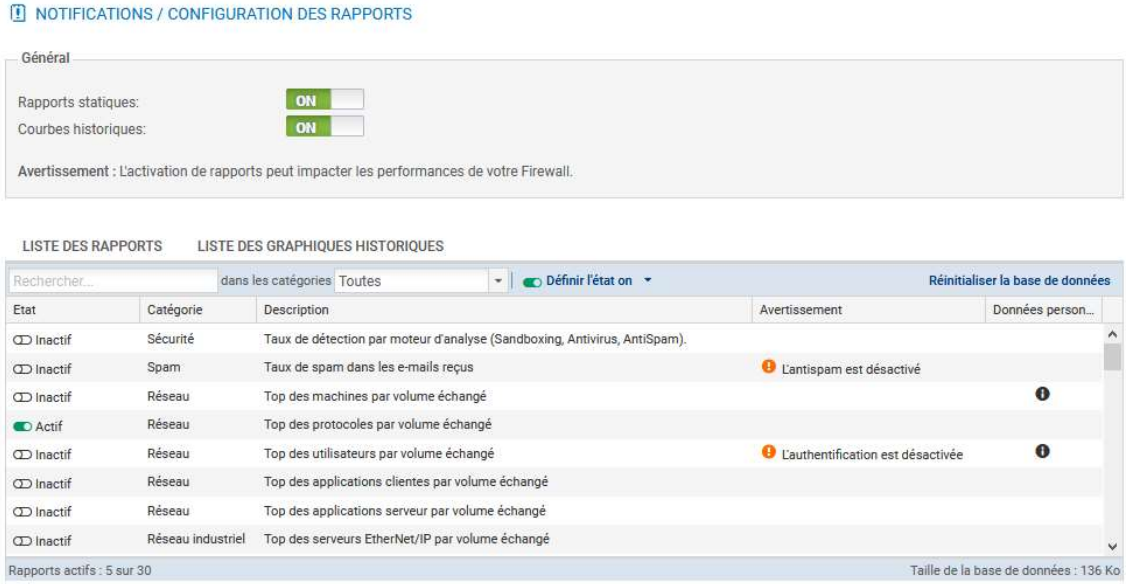
- Le cas échéant, cliquez **Conserver les rapports d'activité désactivés.**

La zone **Configuration de l'espace réservé pour les traces** permet d'activer ou non l'écriture des traces pour une famille donnée en double-cliquant dans la colonne **État** correspondante. Elle permet également de configurer le pourcentage de l'espace disque réservé pour la famille de trace dans la partie **Pourcentage**. Il est important de noter que le total des pourcentages ne doit pas dépasser 100%. La taille réelle de l'espace disque réservé à une famille de traces est indiquée dans la partie **Quota d'espace disque.**

Les entrées de journal anciennes sont écrasées par les nouvelles entrées (rotation) ; il s'agit du comportement par défaut. Pour une journalisation sans rotation, il faut un stockage externe (serveur SYSLOG par exemple).

L'activation des rapports s'effectue depuis le menu **Configuration / Notifications / Configuration des rapports**

Cliquez **Configuration / Notifications / Configuration des rapports** et activez l'option **Rapports statiques**, ensuite sélectionnez les rapports souhaités dans le panneau **Liste des rapports**.



Par défaut le rapport sur le **Top des protocoles** par volume est activé si vous activez les rapports.
L'onglet **Liste des graphiques historiques**, permet de voir et modifier les graphiques qui sont activés par défaut.

1.4 - Traces et Journaux

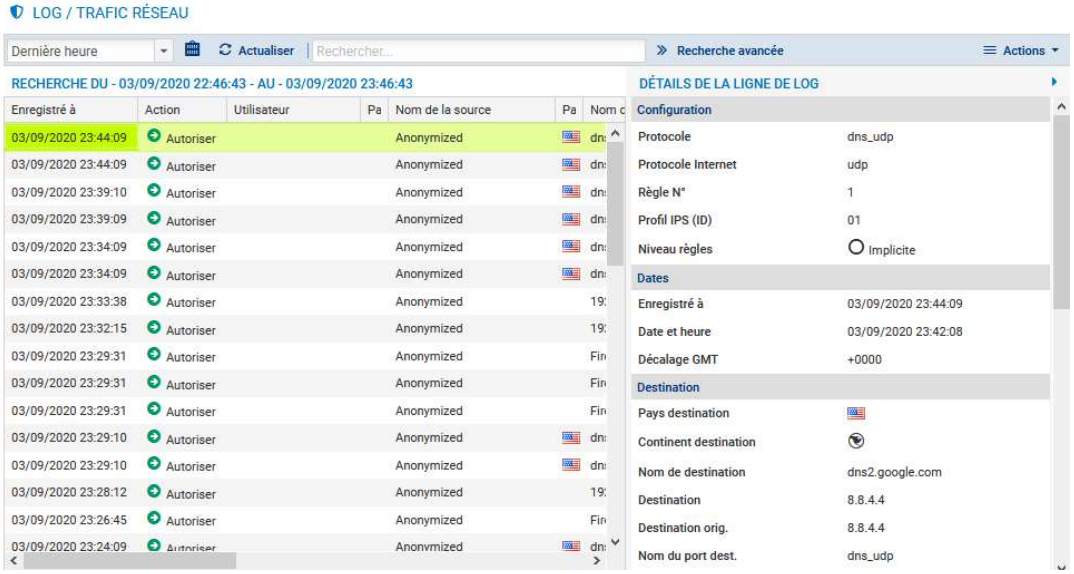
Les fichiers journaux sont organisés en plusieurs catégories décrites ci-dessous.

- **Administration:** Regroupe les évènements liés à l'administration du pare-feu SNS. Ainsi, toutes les modifications de configuration effectuées sur le firewall sont journalisées.
- **Authentification:** Regroupe les évènements liés à l'authentification des utilisateurs sur le pare-feu SNS.
- **Connexions réseaux:** Regroupe les évènements liés aux connexions TCP/UDP traversant ou à destination du pare-feu SNS non traitées par un plugin applicatif.
- **Évènements systèmes:** Regroupe les évènements liés directement au système: arrêt/démarrage du pare-feu SNS, erreurs système, allumage/extinction d'une interface, haute disponibilité, mises à jour Active Update, etc.
- **Alarmes:** Regroupe les évènements liés aux fonctions de prévention d'intrusions (IPS) et les évènements tracés avec le niveau alarme mineure ou majeure de la politique de filtrage.
- **Proxy HTTP:** Regroupe les évènements liés aux connexions traversant le proxy HTTP.

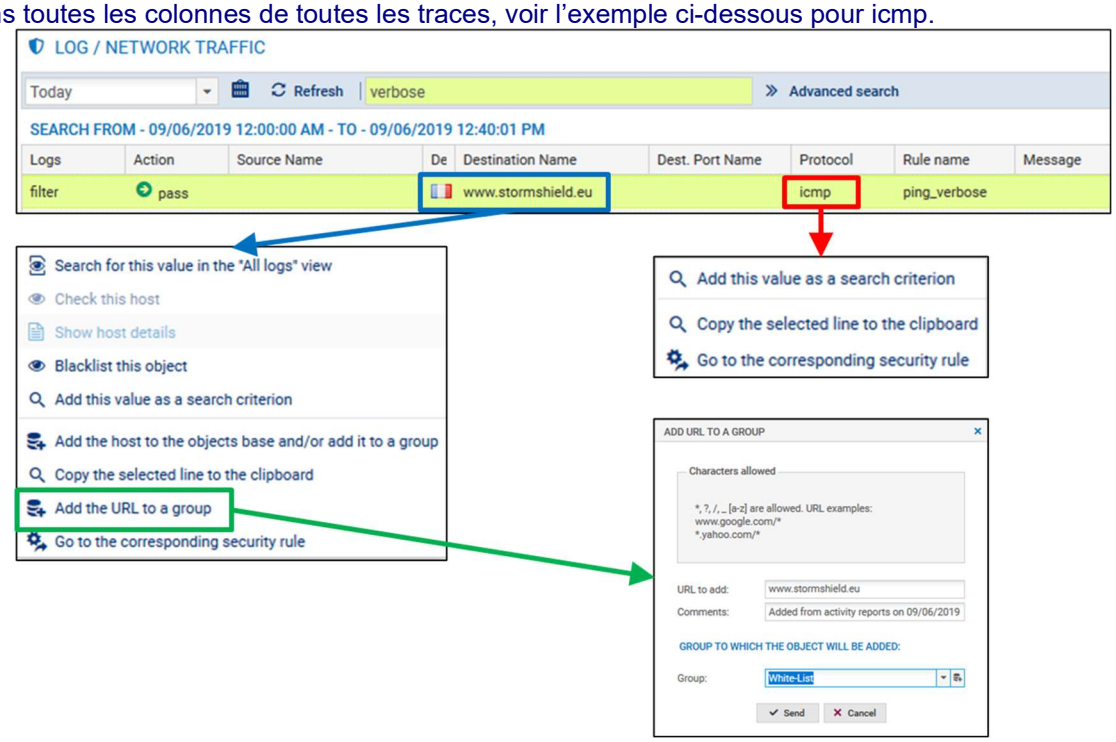
Dans le contexte **Monitoring**, le menu **LOGS - JOURNAUX D'AUDIT** permet de visualiser des traces sauvegardées en local sur le pare-feu SNS, regroupées par famille de journaux : trafic réseau, alarmes, web, etc. Exemple : la famille **Trafic réseau** concatène les journaux : Connexions réseaux, filtrage, Proxy FTP, connexions applicatives, Proxy POP3, Proxy SMTP, Proxy SSL, Proxy HTTP, VPN SSL.
Les traces sont affichées par ordre antichronologique (la trace la plus récente est en tête de liste).
Pour appliquer la nouvelle réglementation européenne sur les données personnelles, le RGPD (Règlement Général sur la Protection des Données), l'accès aux logs des firewalls SNS est restreint par défaut pour tous les administrateurs.
Le super administrateur « admin », ainsi que les administrateurs disposant du droit « Accès aux données personnelles » peuvent accéder aux logs complets en cliquant simplement sur **Obtenir le droit d'accès aux données personnelles (logs)**. Cette manipulation ajoute une entrée dans les journaux qui permet de la tracer.

Cliquez **Monitoring** puis **LOGS - JOURNAUX D'AUDIT** puis **Trafic réseau**

Pour voir l'ensemble des données relatives à une trace, mettez la ligne désirée en surbrillance et cliquez sur la flèche en haut à droite **Détails de la ligne de log**.



L'affichage des journaux peut être restreint à une plage temporelle prédéfinie (dernière heure, aujourd'hui, hier, semaine dernière ou mois dernier) ou personnalisée.
En cliquant sur un type de trace, une fenêtre s'affiche pour offrir des raccourcis vers plusieurs fonctionnalités qui diffèrent suivant le type de trace affichée : afficher de l'aide, ajouter la machine à la base objet, filtrer les traces en se basant sur la valeur, voir la ligne complète de la trace, etc.
Pour **filtrer les traces**, une barre de recherche simple permet de rechercher une chaine de caractères dans toutes les colonnes de toutes les traces, voir l'exemple ci-dessous pour icmp.



Phase 2 Mise en place du plan d'adressage réseau

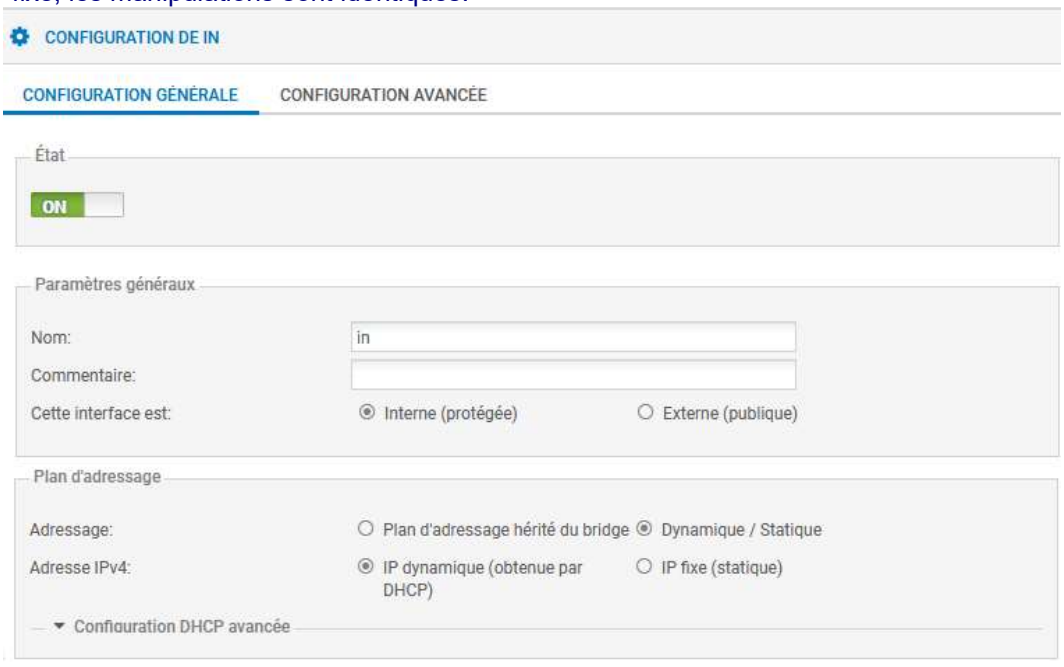
2.1 - Configuration des interfaces réseau

Dans une configuration usine, la **première interface** du pare-feu SNS est nommée « OUT » ou WAN, la **seconde** « IN » et le reste des interfaces « **DMZx** ». L'interface « OUT » est une **interface externe**, utilisée pour connecter le pare-feu SNS à internet (WAN) et le reste des interfaces sont internes et servent principalement à connecter le pare-feu SNS à des réseaux locaux. La distinction interface interne/externe permet de se protéger contre les attaques d'usurpation d'adresse IP.
Pour accéder à l'interface d'administration du pare-feu SNS, il faut connecter votre machine sur une interface interne sous peine d'être détecté comme tentative d'intrusion qui nécessite le redémarrage du firewall.
Nous allons configurer votre pare-feu SNS selon les paramètres de l'architecture globale présentée dans la phase 1 (interfaces IN, OUT et DMZ1) en utilisant le pare-feu SNS en mode « routeur ».
@Interface **OUT** 192.36.253.x0 /24 qui correspond au premier port (WAN)
@Interface **IN** 192.168.x.254 /24 qui correspond au deuxième port (port LAN N°1)
@Interface **DMZ1** 172.16.x.254 /24 qui correspond au port DMZ
@Interface **DMZ2** DHCP qui correspond au port DMZ2 relié à votre LAN interne (BTSSIO).
La **passerelle par défaut** de votre pare-feu SNS sera le pare-feu SNS **Siège** (ou enseignant) **@ 192.36.253.1**.
Pour faciliter la configuration, nous proposons d'effectuer la configuration depuis un poste client connecté à l'interface DMZ2 ou DMZ1 suivant votre pare-feu SNS, que l'on conservera en DHCP sur le réseau interne BTSSIO.
La **configuration des interfaces** s'effectue dans le menu **`Configuration / Réseau / Interfaces`**, en faisant sortir les interfaces Ethernet de l'interface bridge si vous êtes sur un boitier physique ou en VM individuelle.

- **`Configuration / Réseau / Interfaces`**, en faisant sortir les interfaces

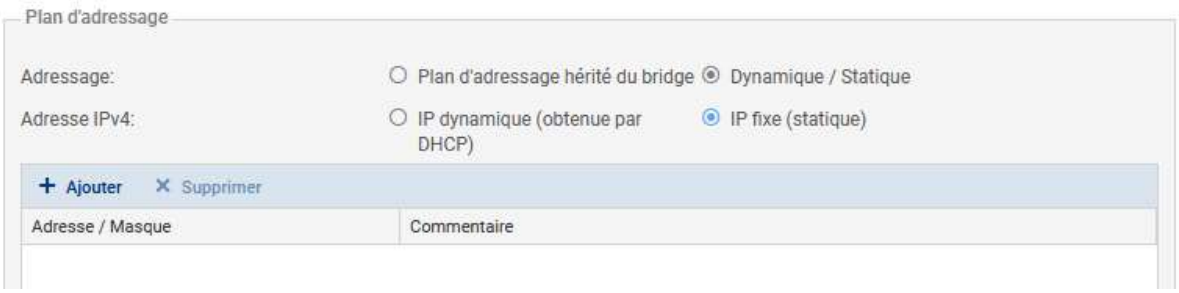
Configuration ferme de serveurs	Configuration boitier avec bridge
	

- Choisir une première interface (par exemple **IN**), pour la sortir du bridge ou la configurer avec une IP fixe, les manipulations sont identiques.



Si l'interface était membre d'un bridge, la configuration est légèrement différente pour la zone **Plan d'adressage** :

- Le cas échéant, Cliquez dans la zone **Plan d'adressage** sur **`Dynamique/Statique`**
- Cliquez **`Ip fixe (statique)`**, un tableau apparaît :



- Cliquez **`+Ajouter`** et dans la zone Adresse / Masque saisissez **l'adresse IP de l'interface IN** 192.168.x.254 puis le masque en CIDR /24 ou en notation décimale pointée : 255.255.255.0

- Cliquez le bouton **`Appliquer`** puis **`Sauvegarder`** et à nouveau **`Sauvegarder`**.

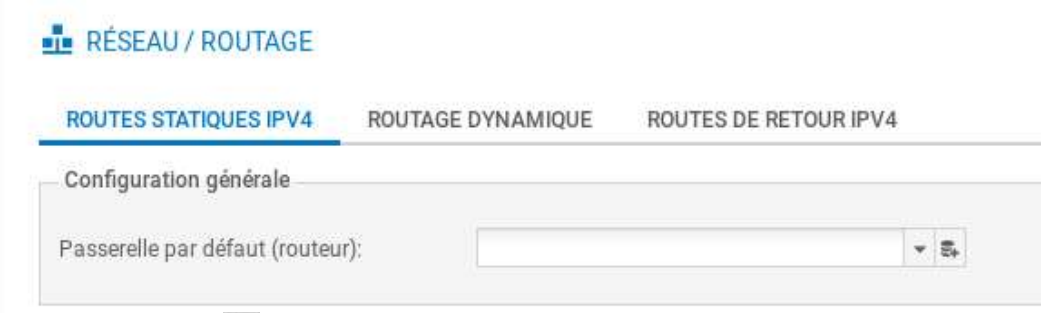
Un message de reconnexion peut s'afficher, le cas échéant reconnectez-vous.

- Procédez de manière identique pour les deux autres interfaces à configurer.

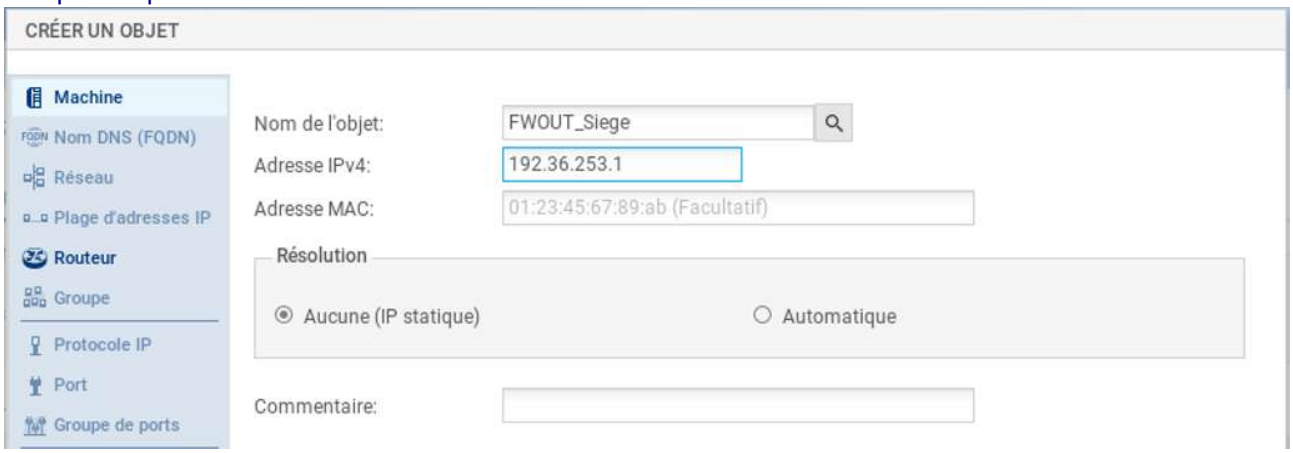
2.2 - Route par défaut

La configuration de la passerelle par défaut de votre pare-feu SNS doit pointer sur l'adresse IP du pare-feu SNS du siège (enseignant) : 192.36.253.1

- Cliquez **`Configuration / Réseau / Routage /`** onglet **`Routes statiques IPv4`**.



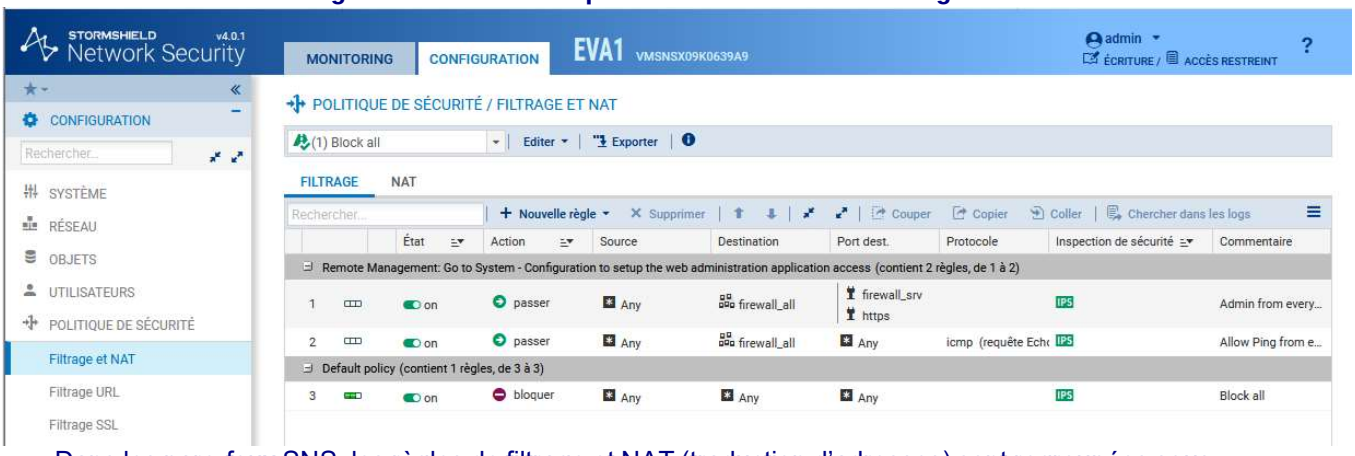
- Cliquez sur le signe pour **ajouter un objet réseau,** choisissez **`Machine`** et renseignez les champs **`Nom`** (Ex : **FWOUT_Siege**) et **`Adresse IPv4`** du pare-feu SNS enseignant : *192.36.253.1* puis cliquez le bouton **`Créer`**.



2.3 - Mise en œuvre de la traduction d'adresses pour l'accès à Internet (NAT/PAT)

Pour ce LAB, nous considérons le réseau externe inter-entreprises comme un réseau public dans lequel aucune adresse IP privée n'est tolérée. De plus, le pare-feu SNS du formateur (SNS Enseignant) est connecté à internet via une interface autre que celles utilisées dans l'architecture du LAB.

- Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage et NAT.`**



Dans les pare-feux SNS, les règles de filtrage et NAT (traduction d'adresses) sont regroupées sous une même politique. Il est possible de définir 10 politiques différentes mais une seule politique est active à la fois, identifiée par l'icône :

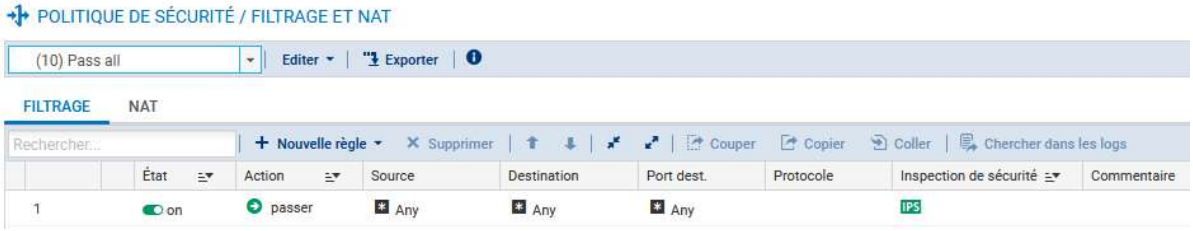
La politique de sécurité active en configuration usine est **(1) `Block all`**, elle n'autorise que le ping des interfaces du firewall et l'accès en https à l'administration du boitier.

Une politique implicite **`Block all`** est également configurée sur le pare-feu SNS.

Pour réaliser les activités, nous allons choisir une politique plus permissive que nous durcirons progressivement.

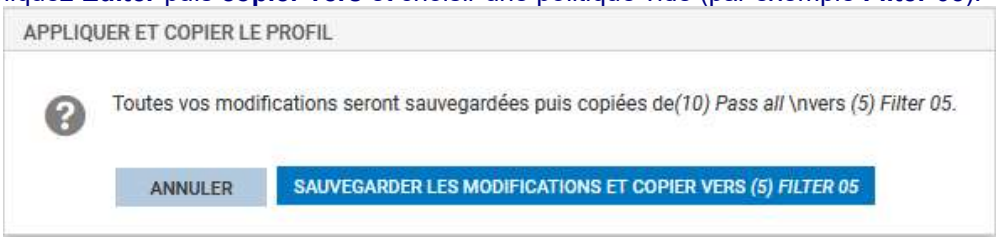
Étape 1 : Copiez la politique de filtrage/NAT (10) **`Pass all`** vers une autre politique vide en la renommant « AgenceX » (remplacez X par la lettre de votre entreprise). Ensuite, **activez cette politique**.

- Dans la liste déroulante des politiques de sécurité, choisissez **(10) Pass all.**



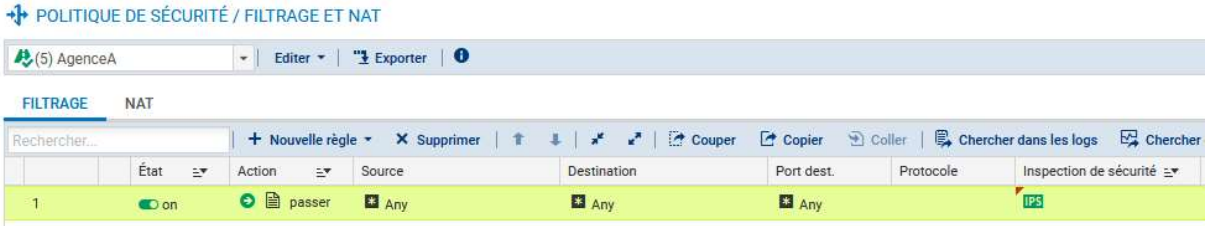
Cette politique laisse explicitement passer tous les flux.

- Cliquez **Éditer** puis **copier vers** et choisir une politique vide (par exemple **Filter 05**).



- Cliquez **Sauvegarder les modifications…**
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée **(05) Pass all.**
- Cliquez **Éditer** puis **Renommer** et renommez-là en « AgenceX », puis **Mettre à jour**.
- Cliquez le bouton **Appliquer** puis **Activer la politique** « AgenceX ».

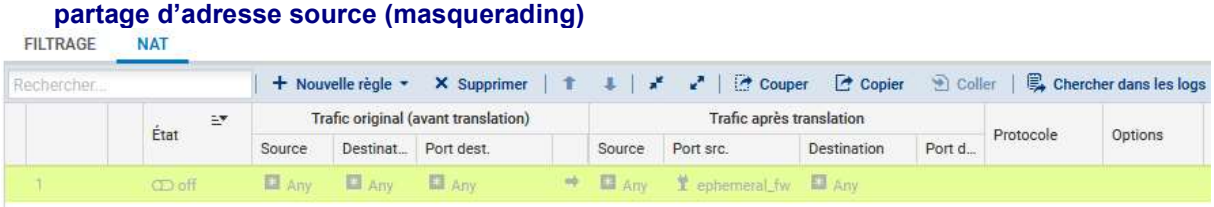
La politique « AgenceX » est activée :



Étape 2 : Ajoutez une règle de NAT afin que les machines de votre réseau interne (**Network_in**) puissent accéder au réseau externe (**Firewall_Out**) sans que leur IP ne soit visible (DNAT). Testez l'accès au réseau externe et l'accès à Internet depuis votre poste sur le réseau interne **IN** de votre agence.

La règle de **NAT dynamique** est créée avec le bouton **Nouvelle règle** / **règle de partage d'adresse source (masquerading)** qui ajoute automatiquement la plage de ports **ephemeral_fw** au niveau du port source dans le trafic après traduction ce qui génère aléatoirement un numéro de port pour chaque nouvelle connexion et la rend moins prédictible.

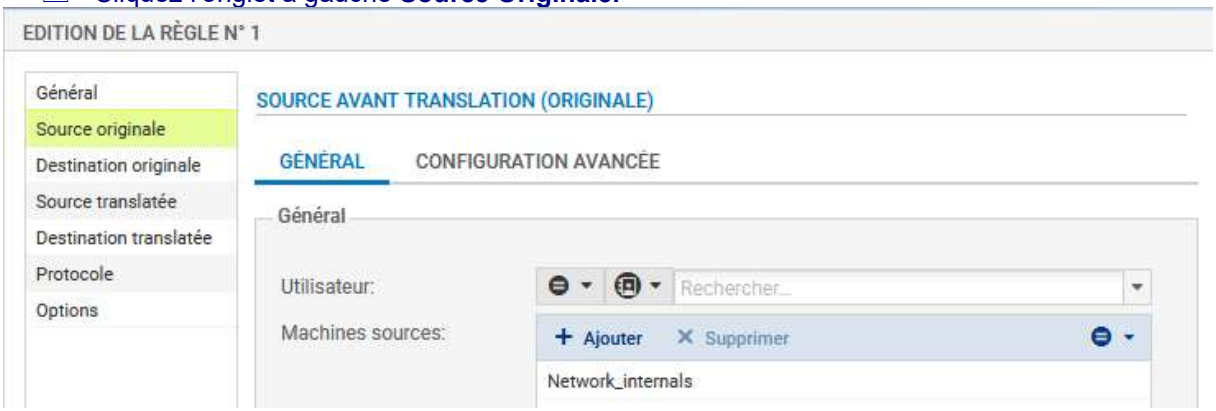
- Dans votre politique **(5) AgenceX**, sélectionnez l'onglet NAT puis **Nouvelle règle** / **règle de partage d'adresse source (masquerading)**



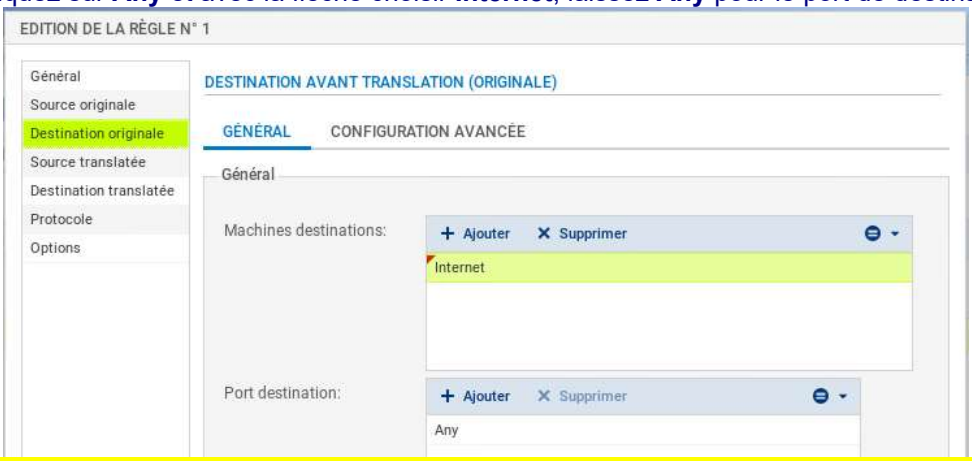
Une nouvelle règle non activée apparaît avec des valeurs par défaut any, any. Dans la section **Trafic après translation**, le port source sera traduit par un numéro de port choisi aléatoirement dans la plage **ephemeral_fw**.

La configuration du **Trafic original (avant translation)** permet de renseigner les valeurs des paramètres avant traduction (par défaut any, any). **Source Originale** permet de définir l'adresse IP d'un hôte ou du réseau source. **Destination Originale** permet de définir l'adresse IP d'un hôte ou du réseau le réseau destination. La configuration du **Trafic après translation** permet de renseigner les nouvelles valeurs des paramètres après traduction (par défaut any, any). **Source** translatée définit l'adresse IP ou le réseau source et le **port** source vus de l'extérieur. **Destination** translatée définit l'adresse IP ou le réseau destination et **Port destination** translatée le port de destination.
Nous allons détailler chaque élément de la configuration de la règle.

- Double-cliquez sur une zone vide de la règle pour ouvrir la fenêtre de configuration détaillée.
- Cliquez l'onglet à gauche **Source Originale.**

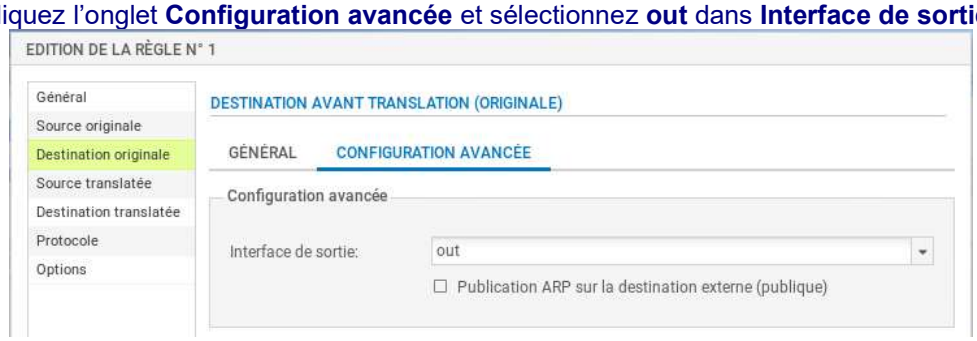


- Cliquez sur **Any** et avec la flèche choisir **Network_internals**, dans l'onglet **Configuration avancée**, laissez **Any** pour le port de destination.
- Cliquez l'onglet du menu de gauche **Destination Originale.**
- Cliquez sur **Any** et avec la flèche choisir **Internet**, laissez **Any** pour le port de destination.

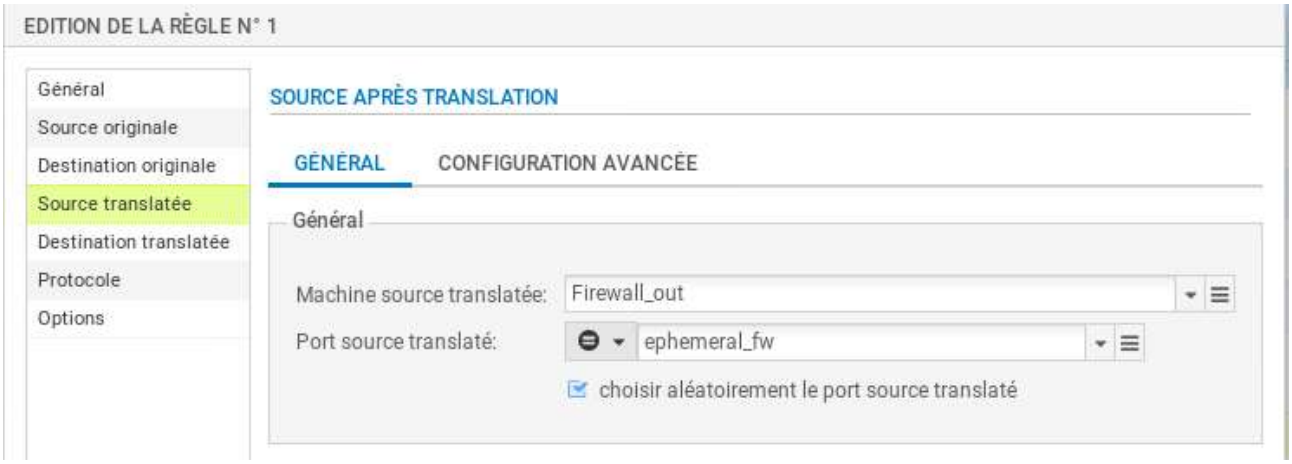


Attention : si vous laissez **Any**, plutôt qu'**Internet** qui désigne tous les réseaux sauf ceux internes au pare-feu SNS, le pare-feu SNS bloquera les flux d'administration (en ssh et en https). En effet, les flux d'administration seront de fait également natés vers l'interface OUT qui l'interprètera comme une tentative d'intrusion et les bloquera.
Vous pouvez sécuriser davantage cette règle en choisissant l'interface de sortie

- Cliquez l'onglet **Configuration avancée** et sélectionnez **out** dans **Interface de sortie**.



- Cliquez l'onglet **Source translatée** et sélectionnez **Firewall_Out** dans **Machine source translatée**.
- Dans **Port source translaté**, laisser **ephemeral_fw** et cochez **choisir aléatoirement le port source translaté**.



- Cliquez l'onglet du menu de gauche **Protocole**, cela permet de définir le type de protocole : applicatif, IP ou Ethernet, laisser **Détection automatique du protocole (par défaut)**

- Cliquez l'onglet du menu de gauche **Options**, cela permet de tracer le trafic qui correspond à la règle de traduction dans le journal de connexions, laissez **standard**.

L'onglet **Options** permet également d'activer le NAT dans le tunnel IPSec (voir VPN IPSec).

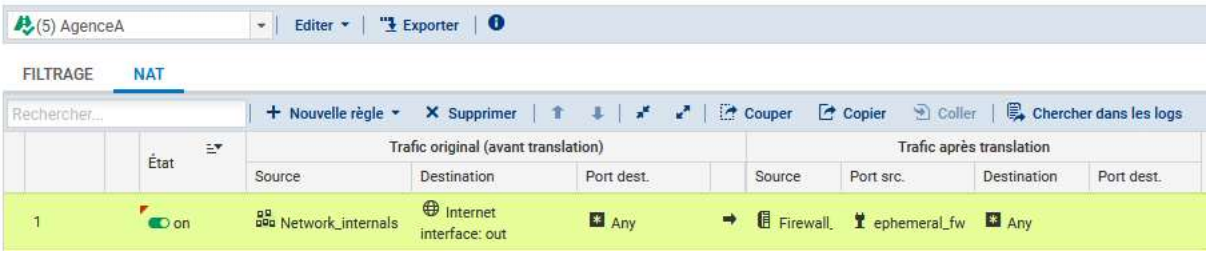
- Cliquez **OK** pour sauvegarder les modifications de la règle de NAT dynamique que vous venez de créer.

- Dans la colonne **État**, sélectionner avec la flèche 

Définir l'état on

La règle passe à 

- Cliquez **Appliquer** puis **Oui, Activer la politique** puis confirmer.



NB : l'accès à Internet est normalement possible via la passerelle de l'enseignant si la traduction PAT est configurée comme ci-dessus.

Pour tester, configurez une machine virtuelle afin d'être dans le réseau interne de votre agence côté interface IN comme suit :

- Adresse IP : 192.168.x.100/24
- Passerelle par défaut : 192.168.x.254
- Serveurs DNS : 172.16.x.10
  et en second le serveur DNS du réseau du BTSSIO ou 9.9.9.9

Effectuez des tests de connectivité vers un serveur extérieur à votre plateforme, par exemple le serveur DNS 9.9.9.9.

NB : le serveur DNS fourni n'effectue la résolution DNS que pour vos adresses locales, elle n'est pas mise en place pour la résolution vers Internet, si vous souhaitez la mettre en place il faut configurer le DNS forwarding.

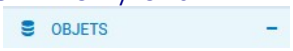
Fiche pratique n°2 : Configuration des Objets Réseau

Dans cette partie, vous allez configurer les objets réseau nécessaires à la mise en place de règles de filtrage et de NAT permettant d'accéder à vos services serveurs en DMZ et à ceux de vos voisins.

Phase 3 Configuration des Objets Réseau

3.1 - Présentation des Objets

Les menus de configuration des pare-feux Stormshield Network utilisent des objets qui représentent des valeurs (adresse IP, adresse réseau, URL, événement temporel, etc.). L'utilisation d'objets au lieu de valeurs présente deux avantages majeurs :
1. Cela permet à l'administrateur de manipuler des noms, plus parlants que des valeurs.
2. Dans le cas où une valeur change, il suffira de modifier la valeur au niveau de l'objet et non dans tous les menus où l'objet est utilisé.
La création et la configuration des objets s'effectuent :

- Dans le menu : CONFIGURATION / OBJETS
- Dans le menu raccourci : 

- Depuis n'importe quel autre menu via le bouton 

  Les objets sont classés en 3 catégories :

  1. Objets Réseau : Regroupe tous les objets en relation avec les valeurs réseaux (adresse IP, numéro de port, numéro de protocole, etc.) et les objets temps.

  2. Objets Web : Groupes d'URL (ou groupes de catégories) et groupes de noms de certificats.

  3. Certificats et PKI : Permet la création et la gestion des autorités de certification et de tous les certificats (de type serveur, utilisateur, ou smartcard) qui en découlent.

Nous nous intéresserons principalement aux objets réseaux. Les objets Web seront abordés dans le chapitre « Filtrage applicatif ». Les objets Certificats et PKI seront abordés dans le chapitre « PKI ».
Lors de la création de la passerelle par défaut, vous avez créé l'**objets Machine FWOUT_Siege.**
La syntaxe des noms des objets doit respecter quelques restrictions définies dans le tableau ci-dessous. De plus, elle est insensible à la casse.

Recommandations :

- suivre une convention de nommage des objets,
- limiter l'usage des objets dynamiques ;
- limiter le nombre d'objets inutilisés ;
- utiliser un groupe d'objet d'administration contenant l'ensemble des IP et des réseaux d'administration permet de réutiliser ce groupe dans toutes les règles de filtrage liées à l'administration et donc de maintenir leur cohérence tout en facilitant leur modification ;
- **éviter les doublons**, c'est une source d'erreur courante lors de la modification de règles de filtrage. On se retrouve dans un cas où la modification d'un objet n'impacte pas toutes les règles qui auraient dû l'être, créant ainsi des trous dans la sécurité.

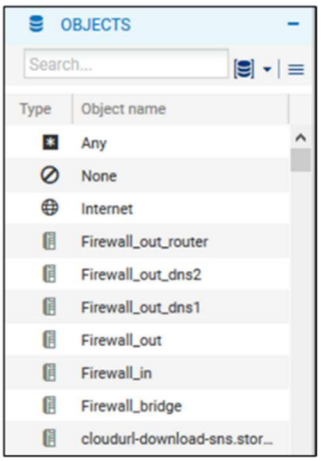
  On peut distinguer deux types d'objets particuliers en plus des objets qui peuvent être créés par l'administrateur :

  • **Objets implicites :** Ils sont créés automatiquement par le firewall et dépendent de la configuration réseau. Ces objets sont en lecture seule et ne peuvent être ni modifiés ni supprimés par l'administrateur. Par exemple, l'objet **« Firewall_out »**, créé automatiquement lorsqu'une adresse IP est associée à l'interface « OUT » ou l'objet **« Network_internals »** qui regroupe tous les réseaux accessibles via les interfaces internes.

  • **Objets préconfigurés :** Ils sont présents par défaut dans la liste des objets. Ils représentent des valeurs de paramètres réseaux standardisées (ports, protocoles, réseaux) et des valeurs nécessaires pour le fonctionnement du firewall (adresse IP des serveurs Stormshield pour les mises à jour). On trouvera par exemple le protocole ICMP et l'objet « **Internet** » ; ce dernier regroupe l'ensemble des machines ne faisant pas partie des réseaux internes.

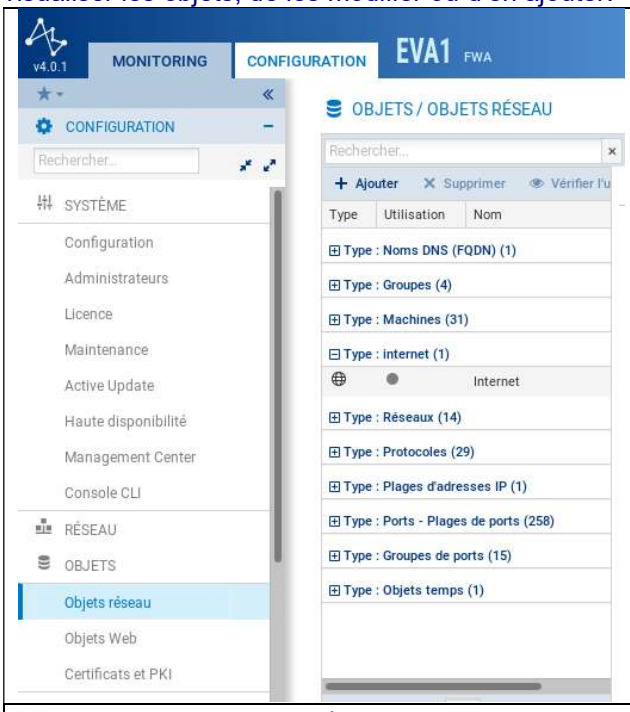
  NOTE : Il est conseillé d'utiliser les objets implicites et préconfigurés et d'éviter de créer d'autres objets portant les mêmes valeurs.

Préfixes interdits	Caractères interdis dans le nom	Noms d'objets interdis	Caractères interdits dans la description
firewall_	<tabulation>	Any	<tabulation>
Network_	<espace>	None	#
Ephemeral_	!	Anonymous	@
Global_	"	Broadcast	"
Vlan_	#	Internet	
Bridge_	,		
	=		
	@		
	[		
	]		
	\		

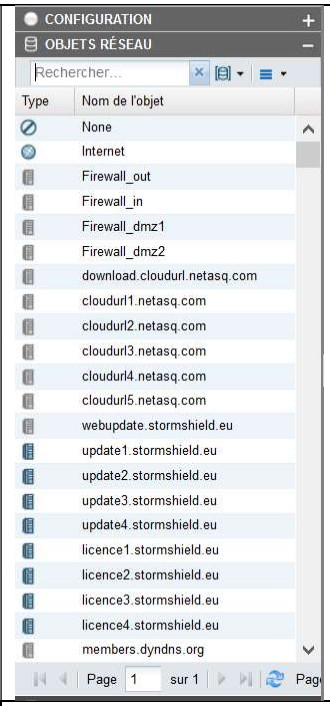


3.2 - Création des Objets Réseaux

Le menu **`Configuration`** / **`Objets`** / **`Objets réseau`** ou le menu **`Objets réseau`** permettent de visualiser les objets, de les modifier ou d'en ajouter.

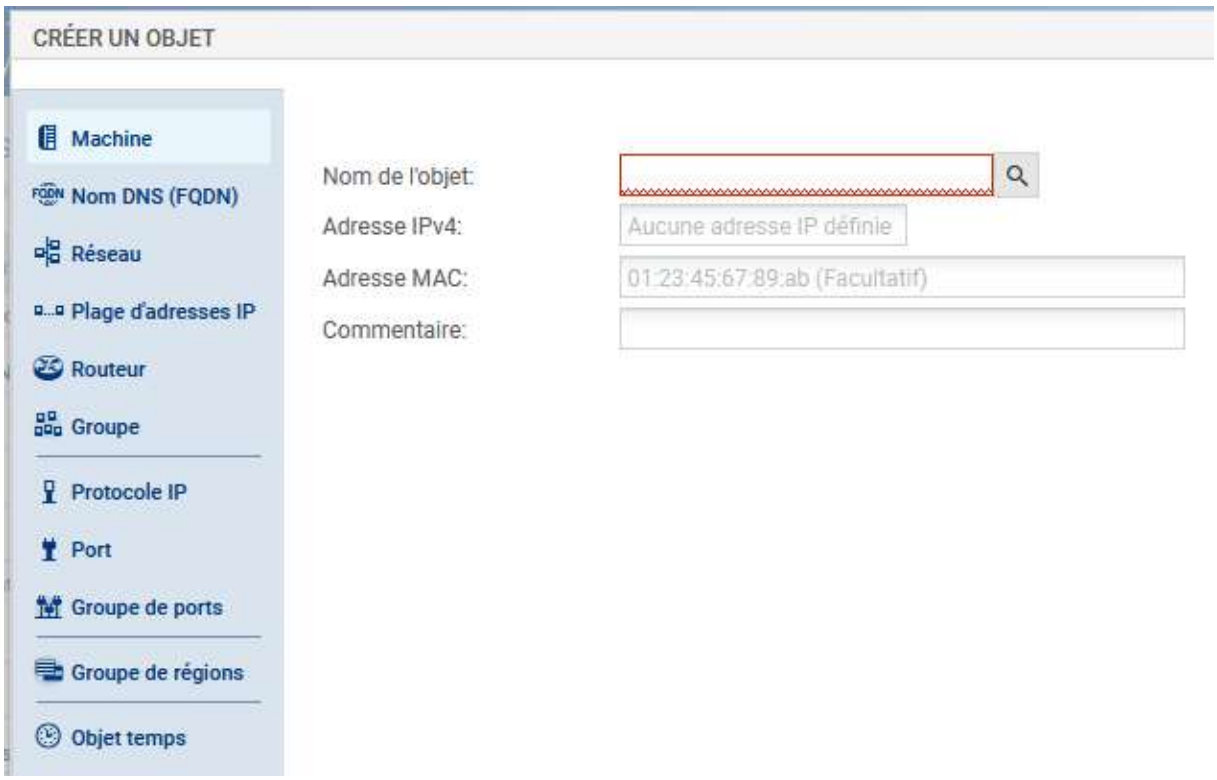


Menu **`Configuration`** / **`Objets`**
Onglet **`Objets réseaux`**



Afficher les objets existants dans la base d'objets réseau

Ouvrez **`Configuration`** / **`Objets`** / **`Objets réseau`** et cliquez le bouton **Ajouter** pour ajouter les objets souhaités.



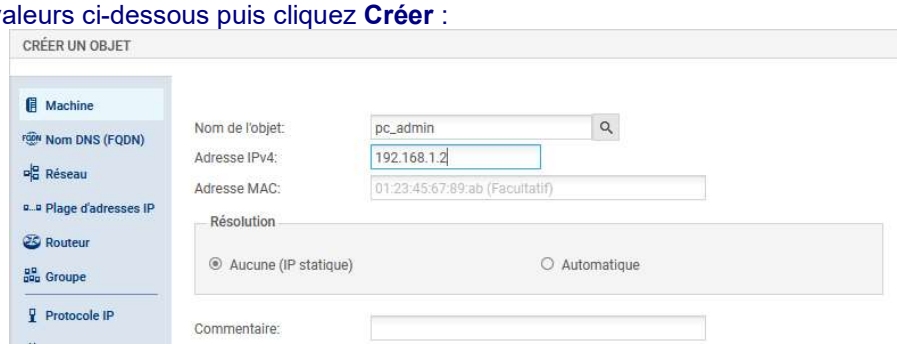
Les types d'objets suivants peuvent être créés :
• **Machine** : Une adresse IP,
• **Nom DNS (FQDN)** : Toutes les adresses IP associées à un nom FQDN par résolution DNS,
• **Réseau** : Une adresse réseau,
• **Plage d'adresses IP** : Une plage d'adresses,
• **Routeur** : Permet de renseigner une ou plusieurs passerelles pour un routage par répartition de charge avec ou sans passerelle de secours.
• **Groupe** : Un groupe d'objets portant une ou plusieurs adresses IP : machines, plages d'adresses IP, réseaux ou d'autres groupes,
• **Protocole IP** : l'ID du protocole au niveau IP,
• **Port - Plage de ports** : Un port ou une plage de ports. Il/Elle peut être limité(e) à un protocole de transport particulier (TCP ou UDP),
• **Groupe de ports** : Un groupe d'objets portant des ports ou des plages de ports, ainsi que d'autres groupes de ports,
• **Groupe de régions** : Un groupe de pays ou de continents. Ce type d'objet peut être utilisé dans la géolocalisation des adresses IP,
• **Objet temps** : Un événement temporel (ponctuel, jour de l'année, jour(s) de la semaine ou plage(s) horaire(s)).
Veillez à utiliser un typage d'objets adéquat (objet réseau pour les réseaux, objet machine pour les pare-feux, etc.).
Note : Dans ce qui suit, le « x » correspond à l'agence considérée, A⇒1, B⇒2, C⇒3, D⇒4, etc.

3.2.1 - Créer des Objets Machines et Réseaux

Vous allez maintenant créer les objets correspondants à vos machines et réseaux internes.

a. Créez un objet **Machine** de nom "pc_admin" avec l'adresse 192.168.x.2

💻 Dans **`Configuration`** / **`Objets`** / **`Objets réseau`** cliquez le bouton **Ajouter** et saisissez les valeurs ci-dessous puis cliquez **Créer** :

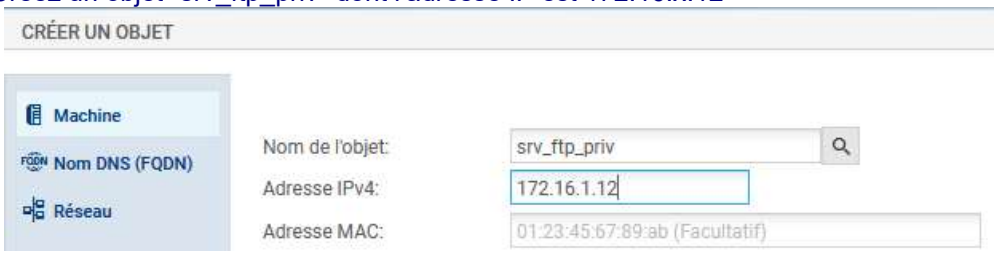


b. Créez un objet "srv_dns_priv" dont l'adresse IP est 172.16.x.10

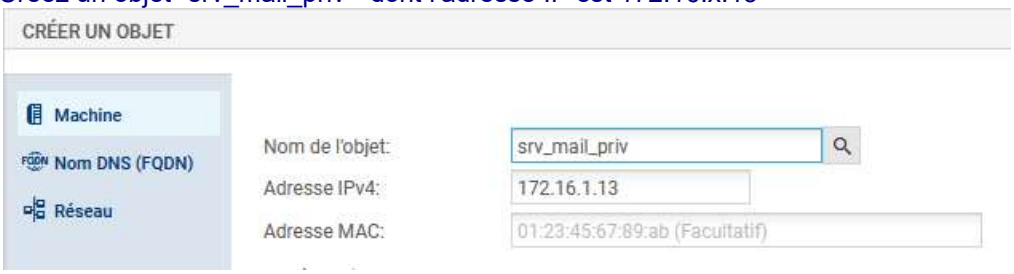
Vous pouvez utiliser le bouton **Créer et dupliquer** pour la création des objets de même type.

c. Créez un objet "srv_web_priv" dont l'adresse IP est 172.16.x.11

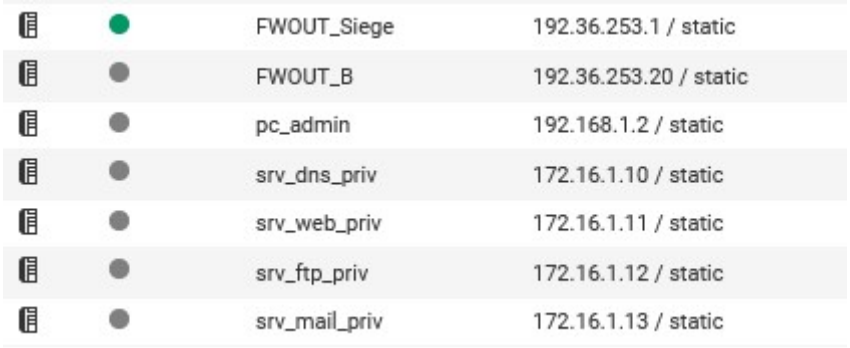
d. Créez un objet "srv_ftp_priv" dont l'adresse IP est 172.16.x.12



e. Créez un objet "srv_mail_priv " dont l'adresse IP est 172.16.x.13

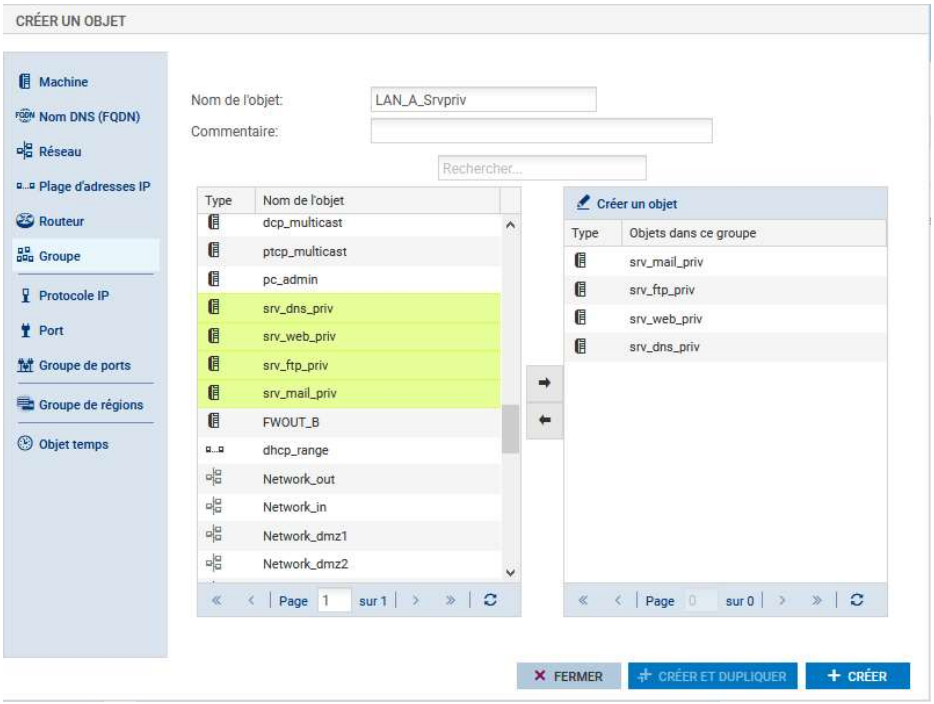


Cliquez la liste **Type** : **Machines** pour déplier et visualiser son contenu.
Vous devez avoir à la fin de la liste des objets **Machines**, les nouveaux objets créés :



f. Créez un groupe d'objets qui contiendra les 4 serveurs que vous venez de définir de nom **LAN_A_Srvpriv**

Cliquez **Ajouter** puis **Groupe,** dans la zone **Nom de l'objet** saisissez **LAN_A_Srvpriv** puis sélectionnez les 4 objets serveurs et à l'aide de la flèche ➡ déplacez les dans la zone de droite **Objets dans ce groupe** puis cliquez **Créer**.

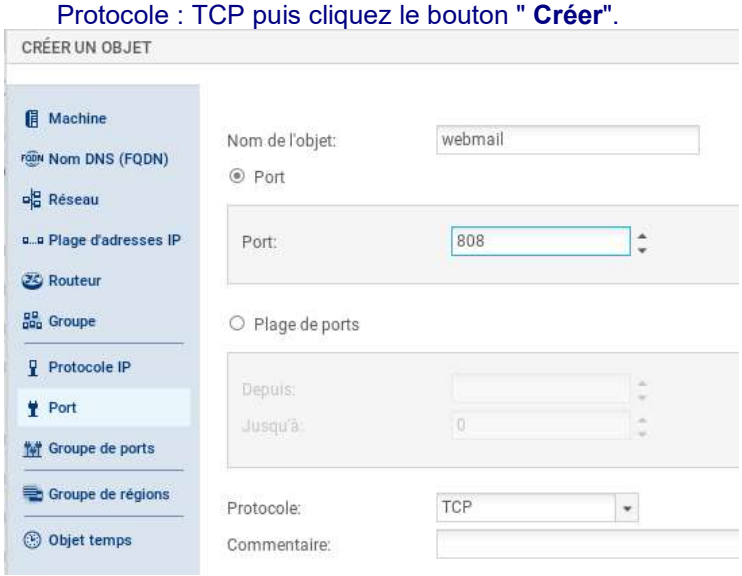


En suivant le même procédé, **créez les objets machines et réseaux** pour l'agence de votre binôme et pour le réseau DMZ du siège :
– Firewalls distants (adresse des interfaces externes), exemple : **FWOUT_x,** en 192.36.253.x0
– Réseaux distants (adresse des réseaux internes), exemple : **LAN_x** en 192.168.x.0 / 255.255.255.0
– Réseau DMZ distant du siège : **DMZ_Siege** en 172.16.250.0 / 255.255.255.0

3.2.2 – Créer un objet Port

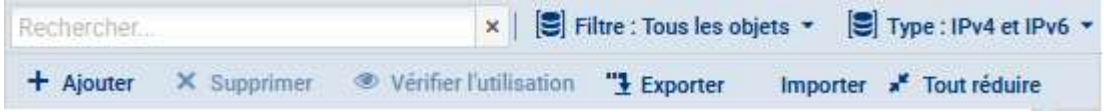
Ajoutez un nouvel objet **Port** basé sur **TCP** fonctionnant sur le port **808**, appelé **webmail**

- Cliquez le bouton "**Ajouter**" « **Port** », choisir le type **Port**, Nom de l'objet : **webmail**, Port : 808, Protocole : TCP puis cliquez le bouton " **Créer**".



3.3 - Import/Export des Objets Réseaux

Vous allez utiliser les boutons **Exporter** et **Importer** pour modifier la base d'objets depuis un fichier csv.



- Cliquez **Exporter**, pour exporter la base d'objets précédemment créés dans un fichier CSV.
- En vous basant sur le format de ce fichier, créez un autre fichier CSV « ObjetsSNSPub.csv » contenant quatre nouveaux objets machines correspondant à l'adresse publique de vos serveurs privés :
  « srv_dns_pub » : 192.36.253.x0

« srv_web_pub » : 192.36.253.x1
« srv_ftp_pub » : 192.36.253.x2
« srv_mail_pub » : 192.36.253.x3
Vous allez importer le fichier CSV dans la base d'objets réseaux.

- Cliquez **Importer**, puis choisissez le fichier « ObjetsSNSPub.csv » et cliquez **Transférer** puis **Fermer**.

NB : En cas de problème à l'importation, encodez le fichier en UTF-8 avec des retours à la ligne type Unix (LF).
Vous devez avoir les nouveaux objets machine dans la liste :

●	srv_dns_priv	172.16.1.10 / static
●	srv_dns_pub	192.36.253.10 / static
●	srv_ftp_priv	172.16.1.12 / static
●	srv_ftp_pub	192.36.253.12 / static
●	srv_mail_priv	172.16.1.13 / static
●	srv_mail_pub	192.36.253.13 / static
●	srv_web_priv	172.16.1.11 / static
●	srv_web_pub	192.36.253.11 / static

- Copiez le fichier CSV ver un nouveau fichier : **ObjetsSNSPub_X.csv**, remplacez les noms et les adresses IP par les adresses IP publiques des machines de votre binôme
  « srv_dns_pub_X » : 192.36.253.y0
  « srv_web_pub_X » : 192.36.253.y1
  « srv_ftp_pub_X » : 192.36.253.y2
  « srv_mail_pub_X » : 192.36.253.y3
- Cliquez **Importer**, puis choisissez le fichier « ObjetsSNSPub_X.csv » et cliquez **Transférer** puis **Fermer**.

●	●	srv_dns_pub_B	192.36.253.20 / static
●	●	srv_ftp_pub_B	192.36.253.22 / static
●	●	srv_mail_pub_B	192.36.253.23 / static
●	●	srv_web_pub_B	192.36.253.21 / static

Les objets ainsi créés seront utilisés dans les règles de filtrage et de NAT.

Fiche pratique n°3 : Configuration de la NAT

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de NAT qui vont permettre d'accéder aux serveurs en DMZ de vos voisins à travers des IP « publiques » ;

Phase 4 Traduction d'adresses (NAT/PAT)

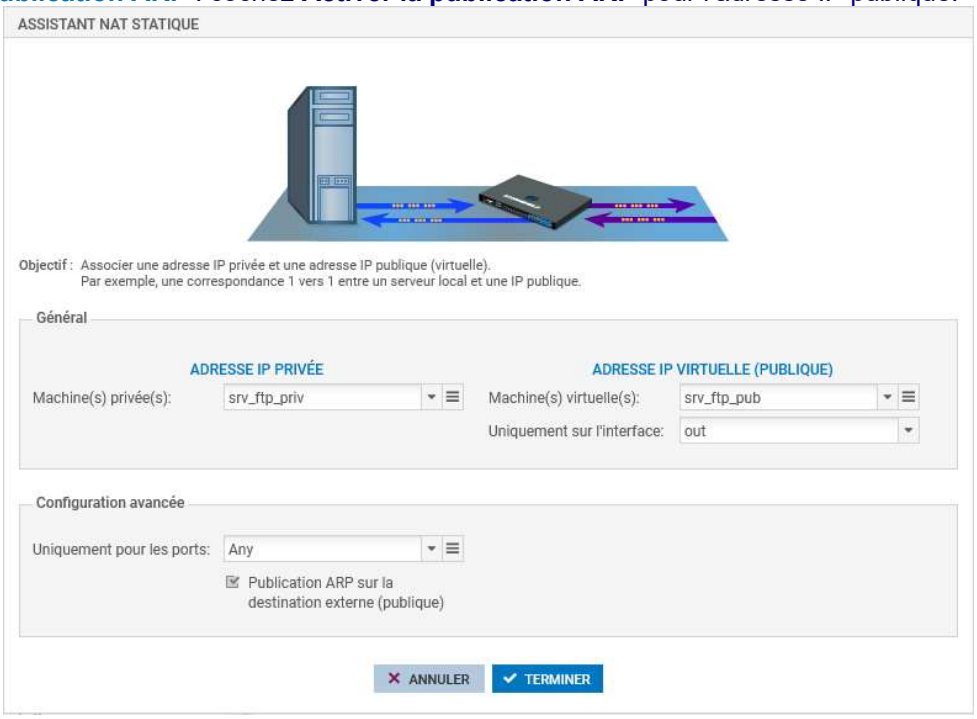
En phase 2 vous avez mis en place une règle de NAT pour permettre l'accès à Internet à vos réseaux internes via la passerelle de l'enseignant.
Nous allons maintenant configurer des règles de NAT et des règles de redirections de ports afin de rendre accessible vos services hébergés par le serveur Debian de la DMZ.

4.1 - Mise en œuvre de la NAT statique

Vous disposez de 2 adresses IP publiques « 192.36.253.x2 » et « 192.36.253.x3 » réservées respectivement à vos serveurs FTP et MAIL (au besoin ajoutez ces 2 objets créés Partie 3).

Étape 1 : Vous allez ajouter les règles de NAT qui permettent de joindre chaque serveur depuis le réseau externe grâce à son adresse IP publique.

- Dans votre politique **AgenceX**, sélectionnez l'onglet **NAT** puis **Nouvelle règle/ règle de NAT statique (bimap)**, un assistant s'ouvre :
  - **Machine(s) privée(s)** : L'adresse IP privée du serveur en interne
  - **Machine(s) virtuelle(s)** : L'adresse IP publique virtuelle dédiée au serveur interne
  - **Uniquement sur l'interface** : L'interface externe depuis laquelle le serveur est accessible avec son adresse IP publique virtuelle.
  - **Uniquement pour les ports** : La règle de NAT statique permet de translater tous les ports, cependant, il est possible de la restreindre en spécifiant un ou une plage de ports au niveau de ce paramètre. Il est conseillé de laisser cette valeur à **Any** et de restreindre le port directement dans les règles de filtrage.
  - **publication ARP** : cochez **Activer la publication ARP** pour l'adresse IP publique.



- Dans **Adresse IP Privée**, **Machine(s) privée(s),** choisissez l'adresse privée de la machine FTP : objet **srv_ftp_priv**.
- Dans **Adresse IP Virtuelle**, **Machine(s) virtuelle (s),** choisissez l'adresse publique de la machine FTP : objet **srv_ftp_pub**.
- Choisissez **out** dans **Uniquement sur l'interface** et laissez **Any** dans **Uniquement pour les ports** et cochez **Publication ARP** et cliquez **Terminer**.

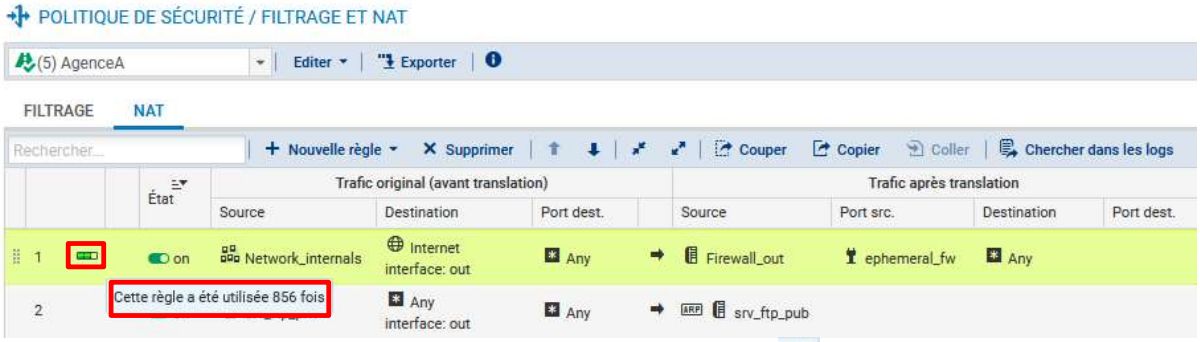
L'assistant ajoute deux règles NATs. La première règle pour la translation du **flux sortant** du serveur interne **vers le réseau public** et la deuxième pour le **flux entrant** à destination de l'adresse IP publique virtuelle. Les deux règles peuvent être modifiées par la suite indépendamment l'une de l'autre.

Procédez de manière identique pour le serveur mail : objet **srv_mail_priv** et objet **srv_mail_pub**

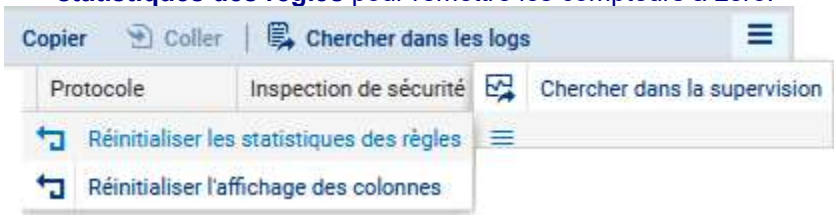
Étape 2 : Testez l'application de la première règle de NAT, en envoyant un ping vers la passerelle par défaut.

Envoyez un ping vers la passerelle par défaut du **Siège** depuis la machine serveur debian du réseau de votre agence (AgenceX)

Ouvrez **Configuration / Politique de sécurité / Filtrage et NAT /onglet NAT** sur le firewall de votre agence (AgenceX). Dans la liste des règles la barre devient verte quand les règles s'appliquent et une info-bulle indique le nombre de fois où la règle a été appliquée :



Dans le bandeau d'affichage des règles, dépliez le menu ☰ cliquez sur **Réinitialiser les statistiques des règles** pour remettre les compteurs à zéro.



4.2 - Mise en œuvre de la redirection de ports

Étape 3 : Vous allez ajouter une règle de NAT afin que votre serveur WEB (objet srv_web_pub, protocole http) soit joignable grâce à une redirection de port via l'adresse IP publique OUT de votre firewall : « 192.36.253.x0 ».

Dans votre politique **AgenceX**, sélectionnez l'onglet **NAT** puis **Nouvelle règle / règle simple**, modifiez avec les paramètres suivants :
Source originale = **Internet**, Intreface d'entrée = **out**, Destination originale = **Firewall_Out**, Port dest= **http**.
Source translatée = **Any**, Destination translatée = **srv_web_priv**, Port destination translaté = **ephemeral_fw**.

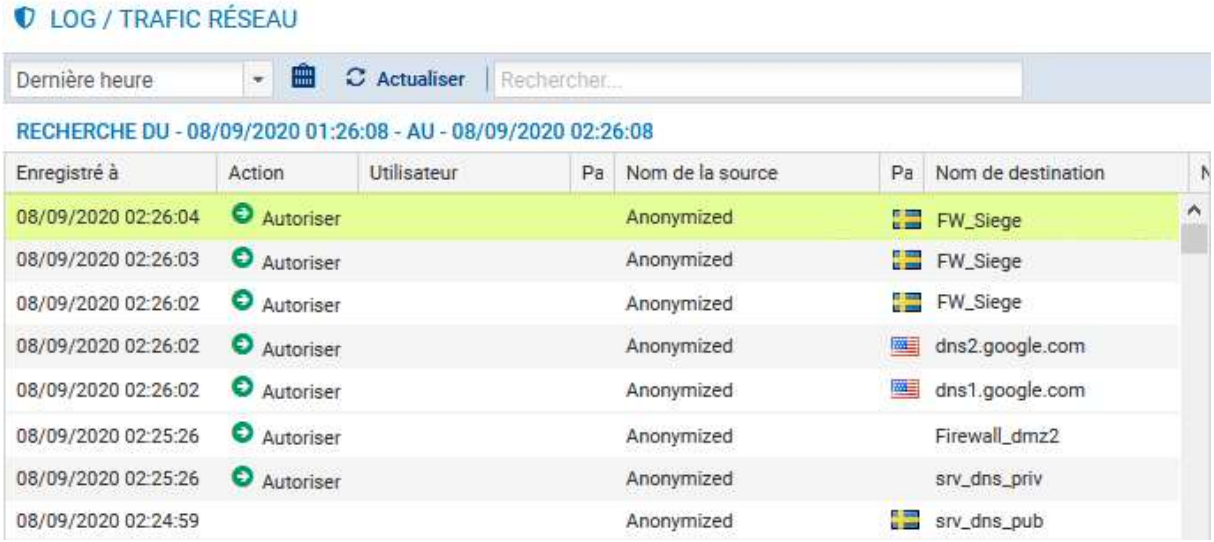
4.3 - Traçage des règles de NAT

Étape 4 : Vous allez activez le traçage des règles de NAT pour les flux entrants, ceci permet d'avoir les informations visibles dans les Journaux d'audit (logs).

Double-cliquez une règle (par ex la règle n°3), et choisissez l'onglet **Options**, et dans niveau de trace **tracer** puis **OK.** Répétez l'opération pour les autres règles **entrantes**.

Vous pouvez tester l'accès à l'ensemble de vos ressources et vérifiez le traçage des règles demandées (flux entrants) dans les logs du firewall. Vous pouvez par exemple tenter d'accéder via des ping d'une machine debian à l'autre.

Cliquez l'onglet **Monitoring** puis **LOGS - Journaux d'audit / Vues / Trafic réseau** : vous devriez voir apparaître les ping vers la passerelle du Siège effectués précédemment.



4.4 - Export des règles de NAT

Étape 5 : Vous allez effectuer une sauvegarde des règles de NAT et de filtrage dans un fichier CSV.

Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage et NAT`**.

Cliquez **Exporter** puis **Télécharger** puis **OK**, le fichier CSV téléchargé est de la forme VMSNSxxxxxxxx_policy5_local_filter_nat_rules_2020-09-08_1731

Fiche pratique n°4 : Configuration du filtrage protocolaire

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de filtrage afin de sécuriser l'accès à votre réseau et interdire certains flux.

Phase 5 Filtrage protocolaire

La mise en place d'une politique de filtrage, permet à l'administrateur de définir les règles qui permettront d'autoriser ou de bloquer les flux au travers de l'UTM Stormshield Network. Selon les flux, certaines inspections de sécurité (analyse antivirale, analyse antispam, filtrage URL, …) peuvent être activées (nous détaillerons ces analyses dans le chapitre « Filtrage applicatif »). Les règles de filtrage définies doivent respecter la politique de sécurité de l'entreprise.

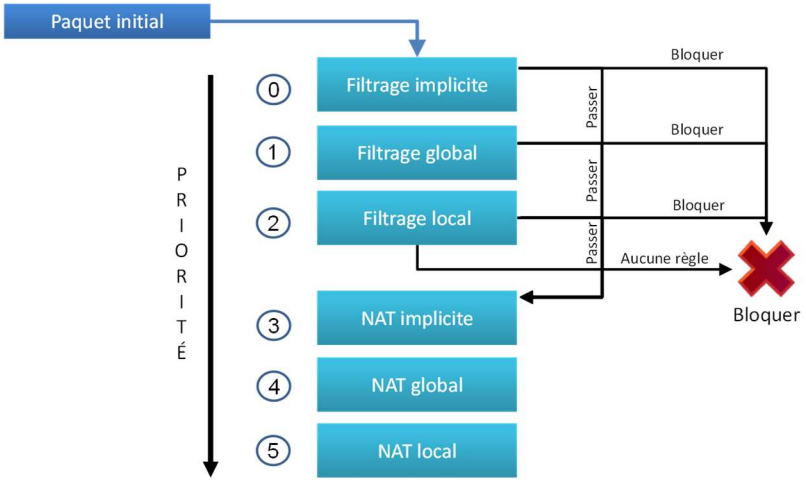
5.1 - Présentation des fonctionnalités

Pour définir un flux, une règle de filtrage se base sur de nombreux critères ; ce qui offre un haut niveau de granularité. Parmi ces critères, il est notamment possible de préciser :

- l'adresse IP source et/ou destination ;
- la réputation et la géolocalisation de l'adresse IP source et/ou destination ;
- l'interface d'entrée et/ou sortie ;
- l'adresse réseau source et/ou destination ;
- le FQDN source et/ou destination ;
- la valeur du champ DSCP ;
- le service TCP/UDP (n° de port de destination) ;
- le protocole IP (dans le cas d'ICMP, le type de message ICMP peut être précisé) ;
- l'utilisateur ou le groupe d'utilisateurs devant être authentifié.

Le nombre de règles de filtrage actives dans une politique est limité. Cette limite dépend exclusivement du modèle de firewall SNS.
Le premier paquet appartenant à chaque nouveau flux reçu par le pare-feu est confronté aux règles de filtrage de la première à la dernière ligne. Il est donc recommandé d'ordonner au mieux les règles de la plus restrictive à la plus généraliste.
Par défaut, tout trafic qui n'est pas autorisé explicitement par une règle de filtrage est bloqué.
Les firewalls SNS utilisent la technologie SPI (Stateful Packet Inspection) qui leur permet de garder en mémoire l'état des connexions TCP et des pseudo-connexions UDP et ICMP afin d'en assurer le suivi et de détecter d'éventuelles anomalies ou attaques. La conséquence directe de ce suivi « Stateful » est l'autorisation d'un flux par une règle de filtrage uniquement dans le sens de l'initiation de la connexion ; les réponses faisant partie de la même connexion sont implicitement autorisées. Ainsi, nous n'avons nul besoin d'une règle de filtrage supplémentaire pour autoriser les paquets réponse d'une connexion établie au travers du firewall.
La figure suivante présente l'ordre d'application des règles de filtrage et de NAT, il est important de noter que les paquets sont filtrés avant d'être « natés » c'est pourquoi nous avons mis au point les règles de NAT avec une politique **Pass all**.

L'ORDONNANCEMENT DES RÈGLES DE FILTRAGE ET DE NAT



Le premier paquet reçu est confronté aux règles de filtrage des différents slots suivant l'ordre présenté dans la figure ci-dessus. Dès que les éléments du paquet correspondent à une règle dans un slot, l'action de la règle (bloquer ou autoriser) est appliquée et le paquet n'est plus confronté aux règles suivantes. Si aucune règle de filtrage ne correspond, le paquet est bloqué par défaut.
Dans le cas où le paquet est autorisé, il est confronté aux règles de NAT des différents slots toujours suivant l'ordre présenté ci-dessus.
Les règles implicites sont accessibles depuis le menu **CONFIGURATION / POLITIQUE DE SÉCURITÉ / Règles implicites**. Chaque règle peut être activée/désactivée.

NB : l*a modification de l'état de ces règles a un impact direct sur le fonctionnement des services du firewall. Pour que le service concerné fonctionne toujours, il faut s'assurer au préalable que le flux est autorisé par les règles de priorité moindre telles que globales ou locales.*

Les règles de filtrage font partie d'une politique présentée précédemment dans le chapitre « Traduction d'adresses ».

Ouvrez le menu **`Configuration`** / **`Politique de sécurité`** / **`Filtrage et NAT`** / **`Filtrage`**
L'onglet **FILTRAGE** est composé d'un en-tête pour la gestion des règles de filtrage :

- Nouvelle règle :
  - **Règle simple** : Ajoute une règle de filtrage standard. Par défaut, une nouvelle règle est désactivée et tous ses critères sont paramétrés à **Any**.
  - **Séparateur – regroupement de règles** : Ajoute un séparateur qui regroupe toutes les règles se trouvant au-dessous (ou jusqu'au prochain séparateur). Cela permet de faciliter l'affichage d'une politique contenant un nombre de règles important. Le séparateur peut être personnalisé par une couleur et un commentaire.
  - **Règle d'authentification** : Démarre un assistant qui facilite l'ajout d'une règle dont le rôle est de rediriger les connexions des utilisateurs non-authentifiés vers le portail captif.
  - **Règle d'inspection SSL** : Démarre un assistant qui facilite l'ajout de règles pour l'activation du proxy SSL.
  - **Règle de proxy HTTP explicite** : Démarre un assistant qui facilite l'ajout de règles pour l'activation du proxy HTTP explicite.
- **Supprimer** : Supprimer une règle.
- **Monter** / **Descendre** : Monter ou descendre la/les règle(s) sélectionnée(s) d'une position dans la liste.

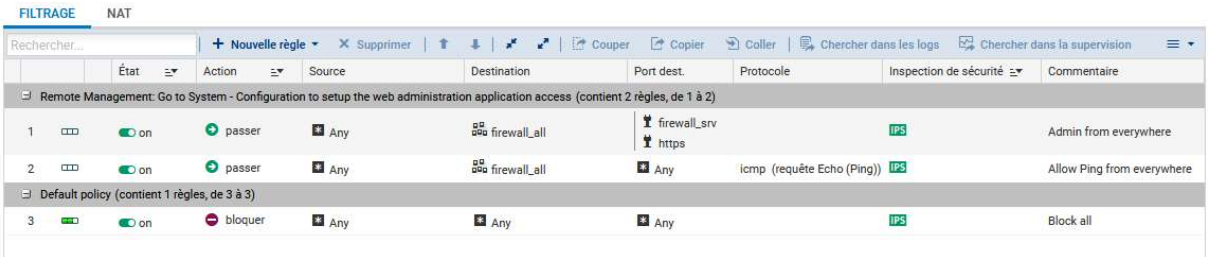
5.2 - Mise en place des règles de filtrage

Vous allez mettre en place une nouvelle politique de sécurité, il faudra commencer par désactiver la règle de filtrage **Pass all** et ajouter les règles de filtrage qui respecteront le cahier des charges décrit ci-après.
Au besoin ajoutez les adresses IP privées de vos serveurs et les IP publiques des serveurs de vos voisins dans les **Objets Réseaux** (cf Phase 3 Objets réseau).

« srv_dns_priv » : 172.16.x.x0 « srv_web_priv » : 172.16.x.x1 « srv_ftp_priv » : 172.16.x.x2 « srv_mail_priv » : 172.16.x.x3	« srv_dns_pub_X » : 192.36.253.x0 « srv_web_pub_X » : 192.36.253.x1 « srv_ftp_pub_X » : 192.36.253.x2 « srv_mail_pub_X » : 192.36.253.x3

Étape 1 : Copiez la politique de filtrage/NAT (1) **`Block all`** vers une autre politique vide où nous allons les copier les règles de NAT de la politique 5.

Dans la liste déroulante des politiques de sécurité, choisissez **`(1) Block all`**.



Cette politique bloque presque tous les flux (règle N°3) sauf ceux définis par les règles 1 et 2.
La règle numéro 1 autorise l'accès en **https** et sur le port prédéfini **1300 firewall_srv** à toutes les interfaces du firewall, elle permet donc l'administration à distance

La règle numéro 2 autorise les requêtes **ICMP Echo** vers toutes les interfaces du firewall, afin de pouvoir vérifier la présence du firewall à l'aide des commandes ICMP.

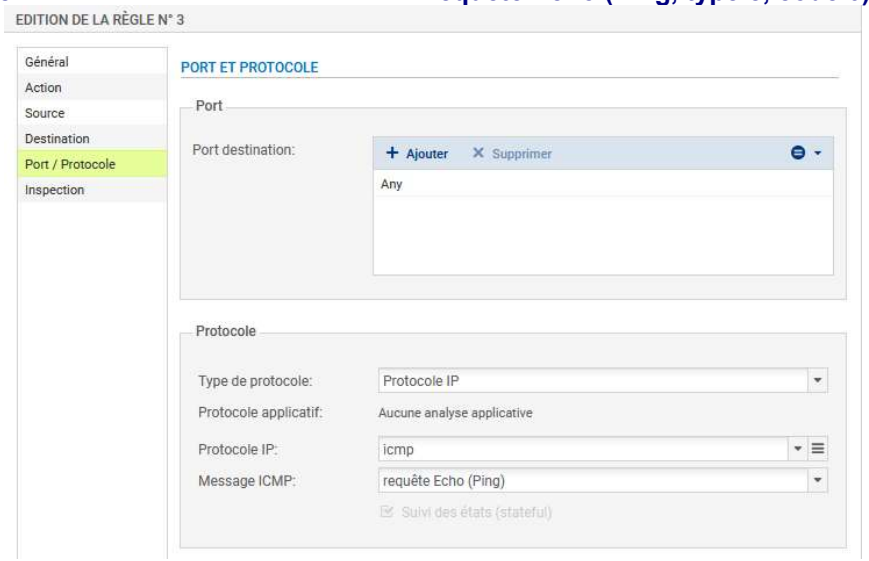
- Cliquez **Éditer** puis **copier vers** et choisir une politique vide (par exemple **Filter 06**).
- Cliquez **Sauvegarder les modifications…**
- Dans la liste déroulante des politiques de sécurité, choisissez la politique copiée **(06) Block all**. Cliquez **Éditer** puis **Renommer** et renommez-là en « **AgenceX_Block all & NAT**», puis **Mettre à jour**.
- Cliquez le bouton **Appliquer** puis **Activer la politique** « AgenceX_Block all & NAT ».
- Dans la liste des politiques de sécurité, choisissez la politique précédente **(05) AgenceX** / onglet **NAT** puis sélectionnez les 6 règles et cliquez **Copier**.
- Dans la liste des politiques de sécurité, choisissez la politique **(06) AgenceX_Block all & NAT** / onglet **NAT** puis cliquez **Coller,** les 6 règles de NAT/PAT sont copiées.

Étape 2 : Nous allons mettre en place une première série de règles sur le Trafic sortant. Nous vous proposons d'utiliser les bandeaux séparateurs en indiquant le rôle de chaque règle pour plus de lisibilité.

a) Votre réseau interne doit pouvoir émettre un **ping vers n'importe quelle destination**.

- Cliquez la règle numéro 2 qui passe en surbrillance et choisissez **Nouvelle règle / séparateur – Regroupement de règle**.

- Cliquez le symbole du crayon et modifiez le nom du séparateur en **ping vers n'importe quelle destination**.
- Cliquez **Nouvelle règle / règle simple**
  - **Action** : **Passer**
  - **Source** : L'adresse IP ou le réseau source, ici **Network_internals**
  - **Protocole dest** : laisser **Any**.
- Double-cliquez sur **Protocole** et remplir les champs comme ci-dessous :
  - **Type de protocole** : **Protocole IP**
  - **Protocole IP** : **icmp**
  - **Message ICMP** : choisir au milieu de la liste **requête Echo (Ping, type 8, code 0)**



La nouvelle règle se présente ainsi :

- Double-cliquez sur le bouton **off** pour passer la règle à l'état **on**, puis cliquez **Appliquer** puis **Oui, activer la politique.**

b) Votre réseau interne doit pouvoir accéder aux serveurs privés de la DMZ (DNS, WEB (ports 80 et 808 pour le webmail), FTP et SMTP).

- Ajoutez un séparateur nommé **Accès aux serveurs DMZ**, choisissez **Nouvelle règle / séparateur – Regroupement de règle** puis éditez-le.
- Cliquez **Nouvelle règle /règle simple**
  - **Action** : **Passer**
  - **Source** : **Network_in**
  - **Destination** : **srv_ftp_priv**
  - **Port dest** : Port destination, ici **ftp**.

Cliquez sur **Copier** puis **Coller** pour créer la deuxième règle à partir de la précédente :

- **Action** : **Passer**
- **Source** : **Network_in**
- **Destination** : **srv_http_priv**
- **Port dest** : Port destination, ici **http**

Cliquez sur **Copier** puis **Coller** pour créer la troisième règle pour le webmail à partir de la précédente :

- **Action** : **Passer**
- **Source** : **Network_in**
- **Destination** : **srv_http_priv**
- **Port dest** : Port destination, ici **webmail** (port **TCP 808**)

Cliquez sur **Copier** puis **Coller** pour créer la quatrième règle pour le serveur mail smtp à partir de la précédente :

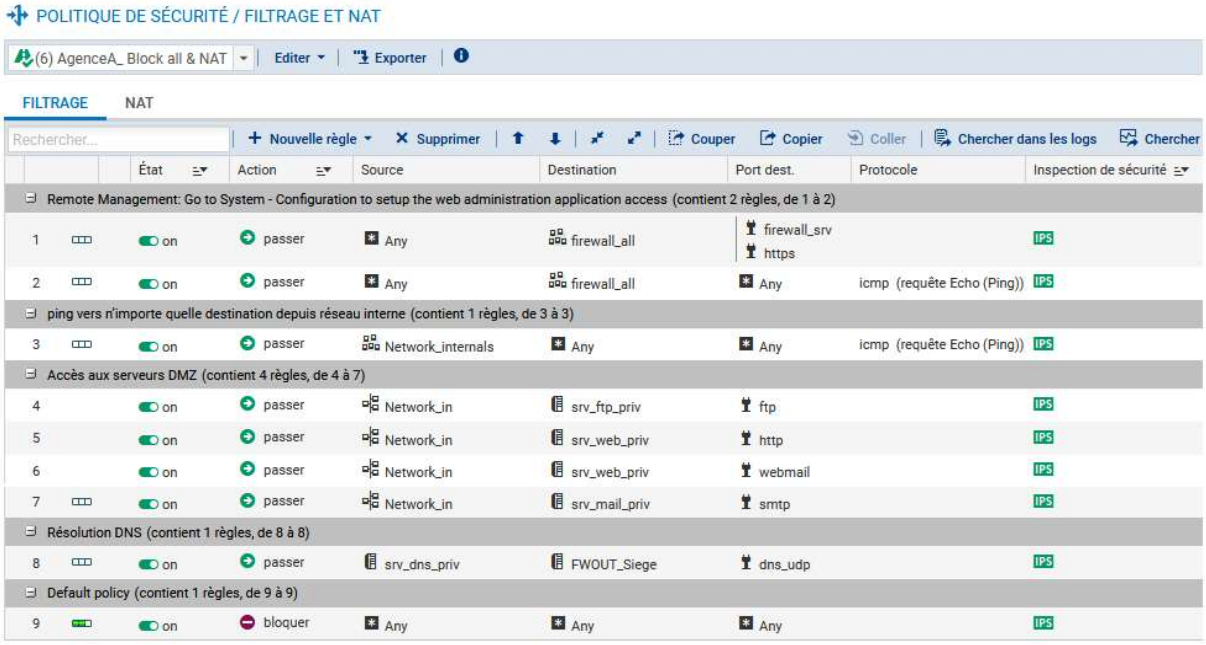
- **Action** : **Passer**
- **Source** : **Network_in**
- **Destination** : **srv_mail_priv**
- **Port dest** : Port destination, ici **smtp**

c) Seul votre serveur DNS interne (172.16.x.10) sera autorisé à résoudre vers l'extérieur, et plus précisément vers l'IP publique du siège (192.36.253.1).

Cliquez **Nouvelle règle /règle simple**

- **Action** : **Passer**
- **Source** : **srv_dns_priv**
- **Destination** : **FWOUT_Siege**
- **Port dest** : Port destination, ici **dns_udp**.

Double cliquez sur le symbole **off** des règles pour les passer à l'état **on**, puis cliquez **Appliquer** et **Oui, activer la politique.**
Les règles actuellement mises en place sont les suivantes :



Étape 3 : Vous allez mettre en place une deuxième série de règles sur les trafics entrants et sortants qui respecteront le cahier des charges ci-dessous (utilisez les séparateurs en indiquant le rôle de chaque règle).

Trafics sortants :

1. Votre réseau interne (DMZ incluse) doit pouvoir joindre les serveurs FTP et Web de vos voisins.
2. Un stagiaire, nouvellement arrivé dans l'entreprise, a l'interdiction d'effectuer la moindre requête FTP. L'adresse IP de sa machine est 192.168.x.200.
3. Votre serveur de messagerie peut envoyer des mails vers les serveurs publiés par vos voisins.
4. Votre réseau interne, à l'exception de vos serveurs en DMZ, doit pouvoir naviguer sur les sites web d'Internet en HTTP et HTTPS, sauf sur les sites de la République de Corée (test avec www.visitkorea.or.kr).
5. L'accès au site https ://www.cnn.com doit être bloqué depuis le réseau interne, en utilisant un objet FQDN.

Trafics entrants :

6. Les voisins et le formateur peuvent joindre vos serveurs Web et FTP ; ces événements doivent être tracés.
7. Les serveurs mails voisins sont autorisés à transmettre des e-mails à votre serveur de messagerie
8. Les voisins sont autorisés à pinger l'interface externe de votre SNS ; cet événement devra lever une alarme mineure.
8. Le formateur est autorisé à pinger l'interface externe de votre SNS.
9. Les voisins et l'enseignant peuvent se connecter à votre SNS : via l'interface web et en SSH. Ces événements devront lever des alarmes majeures.

Fiche pratique n°5 : Configuration du filtrage applicatif

Dans cette partie, vous allez reprendre l'architecture présentée dans la fiche N°1 et mettre en place des règles de filtrage au niveau applicatif afin de mieux sécuriser l'accès à votre réseau : interdire certains flux applicatifs, contrôler l'accès aux sites web, prévenir les tentatives d'intrusion…

Annexe – Procédure de Remise à zéro des Pare-feux SNS

Un RAZ du firewall peut être fait via la console (sur les VM ou les boitiers physiques), ceci nécessite un redémarrage (reboot). C'est l'équivalent d'un appui sur le bouton reset pour les boitiers physiques.
Nous effectuons cette opération afin de pouvoir démarrer les machines virtuelles sur une ferme de serveurs avec un vlan commun à tous les pare-feux reliant leurs interfaces OUT.
Dans la configuration par défaut des VM du laboratoire Stormshield, toutes les interfaces appartiennent à un « bridge » et ont la même adresse IP, ce qui fonctionne avec des boitiers physiques ou avec les labs individuels sur virtualbox mais génère du trafic que le pare-feu va bloquer en le reconnaissant comme une tentative d'intrusion.
La remise-à-zéro va consister dans un premier temps à supprimer le bridge et mettre des adresses en DHCP (ou fixes) pour faciliter le paramétrage ensuite par l'interface web.

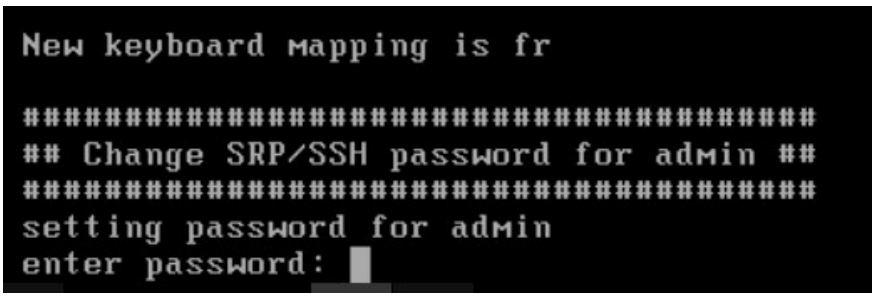
- Démarrez la machine virtuelle ou le boitier et accédez à la console en administrateur
- Tapez la commande **cleanfw -c**

```
VMSNSX09K0639A9>cleanfw -c
Kill all test process
Remove local backup (autobackup)
Remove previous faulty fwtest traces...
Restore default configuration
Restoration done, reboot recommended
Clear History
VMSNSX09K0639A9>
```

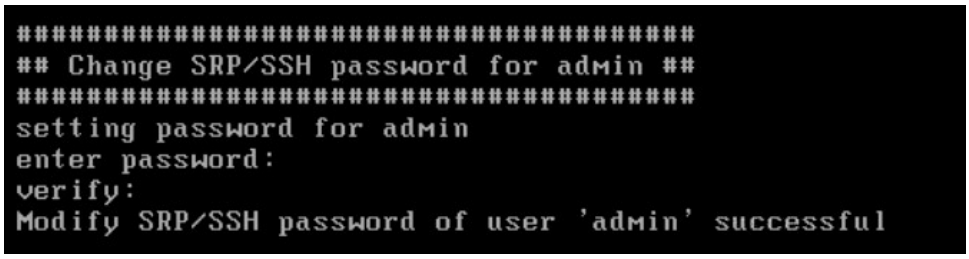
- Redémarrez la machine virtuelle à l'aide de la commande **reboot** et répondez aux questions de configuration initiale

```
Pattern checking...Done

Starting daemons... logd monitord hardwared asqd userreqd modem service dns ldap
 voucher filter network dialup ha snmp bird ipsec sl openvpn antivirus dhcp ntp
smcrouting event cad thind alived telemetryd.
Setting boot partition to Main
No BACKUP partition found
mount_cd9660: /dev/cd0: No such file or directory

################################
## Configure keyboard mapping ##
################################

Current keyboard mapping: us.iso

The available choices are:
        1 - ch
        2 - de
        3 - es
        4 - fr
        5 - it
        6 - pl
        7 - us
Select your keyboard mapping number:
```

  - ⇨ Sélectionner 4 pour fr

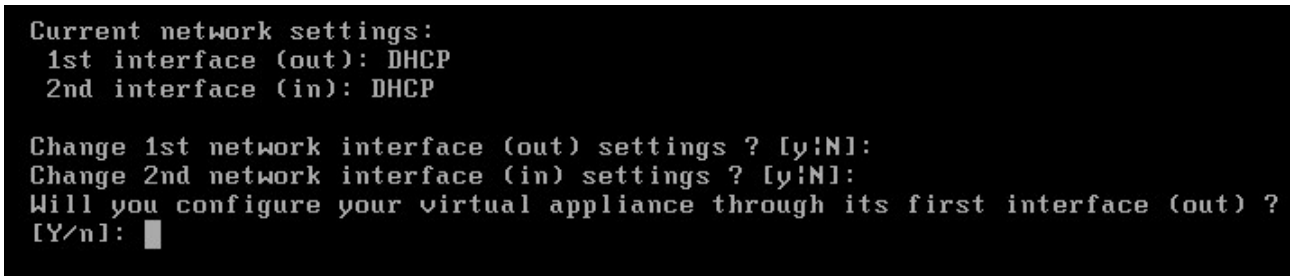


⇨ Entrez un mot de passe de 8 caractères minimum avec Maj/min, pour éviter les soucis de clavier américain, entrez SioSioSio puis confirmez

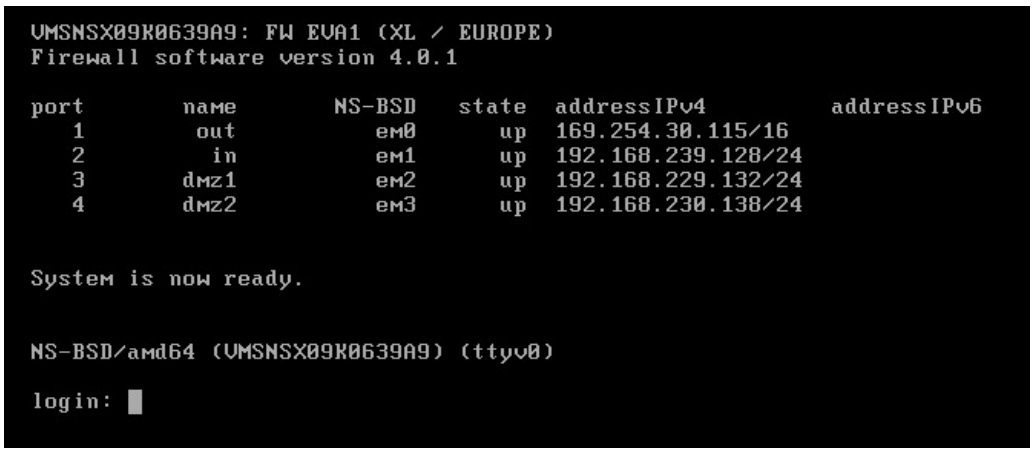


Passons à la configuration des interfaces réseau :

⇨ Pour ce premier démarrage on va laisser les interfaces en DHCP, répondre N ou Entrée même si aucun serveur DHCP n'est relié à ces réseaux.



⇨ Répondre N, en effet il n'est pas recommandé d'autoriser l'administration sur votre interface OUT



Votre système est installé avec les valeurs rappelées ci-dessus, vous pouvez tester que la configuration du clavier a bien été prise en compte en saisissant votre login/mdp.